PRIVACY WITHIN THE PRIVATE ORDER: A CRITICAL EVALUATION OF THE MARKET-BASED SYSTEM GOVERNING DATA COLLECTION IN THE UNITED STATES

Claire McCloskey[*]

Abstract: This paper critically evaluates the market-based system governing data collection in the United States. The discussion is centred around Big Tech, a group of information intermediaries responsible for the ongoing extraction and exploitation of consumer data. The exploitative system is enabled by the ubiquitous privacy policy, which ostensibly offers data subjects 'notice' of data collection and the 'choice' to consent to said collection. This paper critiques the 'notice' and 'choice' model, noting the combined ambiguity and opacity of the privacy policy fails to offer subjects meaningful control over their data. To substantiate this argument, the paper evaluates the suitability of the market-based system in a broader sense, arguing that data collection practices precludes the knowledge parity necessary for an operative and fair market-based system. The paper concludes by ascertaining the suitability of state-based regulation, identifying data's intrinsic relationship with ideals that are core to the Western tradition: equality, democracy, and autonomy.

A. INTRODUCTION

Information technology has become a ubiquitous force in the 21st century.[1] A collection of corporations, namely Facebook, Amazon and Google which fall under the hypernym of 'Big Tech', have pioneered this movement, wielding consumer data as their primary resource. A balancing exercise between consumer privacy and commercial bifurcation subsequently ensues.[2] Providing the epicentral infrastructure by which global connectivity, commercial activity and information discovery is proliferated, the technological collective asserts dominance in both the market and civic society.[3] In light of this power, privacy concerns have arisen, the emphasis being on the alleged invasive and exploitative nature of data extraction.[4]

Privacy discourse exhibits two schools of opposing thought. Neoliberal dialogue, which holds that corporations should remain unregulated as to grant the consumer ultimate autonomy

[*] LL.M. with Distinction in International Commercial Law (University College London), LL.B. (Durham University). All errors and omissions are my own.

[1] Rana Foroohar, *Don't Be Evil: The Case Against Big Tech* (1st edn, Allen Lane 2019).
[2] David E. Pozen, 'Privacy-Privacy Tradeoffs' (2016) 83 U Chi L Rev 221, 247.
[3] Foroohar (n 1).
[4] Adam D. Moore, 'Toward Informational Privacy Rights' (2007) 44 San Diego L Rev 809, 812.

 DOI: https://doi.org/10.14324/111.444.2052-1871.1207.

in his data transactions,[5] dominates one side of the regulatory debate. Critics of this view often support state-based regulation, maintaining that the market-based system does little to protect the individual consumer from abuse and manipulation.

The regulatory system governing Big Tech in the United States (hereafter US) is largely enabling to the former notion. Big Tech, through the manipulation of market rules and self-regulatory principles, possesses significant discretion within the system. The American stance contrasts with other systems such as the European Union (hereafter EU), with its rights-based conceptualisation of privacy[6] and corresponding legislation. The organisational concentration of Big Tech within the US, and the extra-territorial effect of American regulatory culture, has the potential to generate not only domestic privacy concerns, but also concerns beyond national borders. Consequently, the efficacy of the US regulatory system is of critical importance to data subjects worldwide.

This paper evaluates the sufficiency of US market-based regulation governing data collection. It scrutinises the market and its rules, concluding it is a wholly unsuitable framework for privacy protection. Big Tech's bargaining power and the subsequent manipulation of the user undermines the purpose of the market in its goal to engender autonomy and liberty of all actors. The paper will subsequently ascertain that such insufficiencies qualify the imposition of state-based regulation, ensuring the protection of the individual consumer.

The first section will study privacy in a broad sense, exploring both cultural attitudes and the system purportedly protecting privacy. This exploration highlights the backdrop against which contemporary notions of privacy have evolved and will serve to contextualise the paper's subsequent arguments. The second section will analyse the self-regulatory system itself, focusing on the inadequacies of the Fair Information Practice Principles, the 'notice and choice' model and the competency of the Federal Trade Commission (hereafter FTC) in regulating data collection. This critical analysis will form the basis of the paper's disapproval of the current self-regulatory system. The third section, in drawing on economic, regulatory, and ethics-based commentary, will explore the suitability of the market-based system more generally, concluding its application to privacy-related concerns is wholly undesirable. The paper will expand on the preferred mode of state-based regulation, suggesting that an enforceable system of law offers greater protection for ideals central to Western civic society.

[5] Luca Belli, 'Private Ordering and The Rise of Terms of Service as Cyber-regulation' (2016) 5(4) Internet Policy Review 1, 17.
[6] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale LJ 1153, 1165.

B. THE CURRENT MARKET-BASED SYSTEM REGULATING BIG TECH'S PROTECTION OF PRIVACY

1. Defining Privacy

Those who attempt to define privacy will face a nebulous, ill-defined wealth of information. The initial concept of privacy emanates from Warren and Brandeis' hypothesis on the 'right to be let alone'.[7] However, the term has gained greater traction with Westin's 'Privacy and Freedom'.[8] In conceptualising four variations of privacy: solitude, anonymity, reserve, and intimacy,[9] Westin expanded privacy's theoretical boundaries, facilitating adaptation to contemporary data-related understandings.

In coalescing Westin's four strands of privacy, a 'privacy-as-control' definition shall be assumed for the purposes of the paper, which asserts that privacy is 'the control we have over information about ourselves.'[10] Moore has expounded on the definition extensively,[11] noting its applicability and suitability for US techno-privacy matters. This definition can also be reconciled with free-market theory's application to privacy, wherein individuals are encouraged to embark on privacy self-determination. Within the endogenous community, the onus is placed on the individual to organise their affairs when 'negotiating' and 'bargaining' with information intermediaries.[12]

2. The Current Regulatory Framework

This section explores the rules, both persuasive and authoritative, that govern corporations' use of data. The system is distinct from that governing general corporate activity, in which firms are ordered by state legislation.[13] With regards to data collection, corporations operate within a market-based system; rules exist as voluntary principles and 'soft law', granting information intermediaries significant discretion when managing consumer data. Notably, the differential treatment enjoyed by Big Tech is recognised by the companies themselves. In Google and Facebook's S-1 Registration Statements, their respective founders claim, 'Google is not a

[7] Pozen (n 2) 226.
[8] Lisa Austin, 'Re-reading Westin' (2018) 20(1) Theoretical Inquiries in Law 53, 53.
[9] ibid 54.
[10] Charles Fried, 'Privacy' (1968) 77 Yale LJ 475, 482.
[11] Moore (n 4).
[12] Daniel Attenborough, 'Empirical Insights Into Corporate Contractarian Theory' (2017) 37 Legal Stud 191,193.
[13] Facebook, Google and Amazon are incorporated in Delaware, and are thus subject to the force of the Delaware General Corporation Law. See David A. Skeel, Jr., 'Icarus and American Corporate Regulation' (2005) 61 Bus Law 155, 167.

conventional company',[14] and 'Facebook was not originally created to be a company, [but] a social mission'.[15]

The anti-statist position originates from the Chicago School, in which neoliberal economists eschew intensive state intervention.[16] As a founding member of the School, Friedrich Hayek elucidates the enabling power of the market in engendering liberty.[17] In a polemic against dirigisme, Hayek stresses the falsity of the 'collective freedom' purportedly provided by intervention. His account of the market prioritises individual autonomy, where the actor is free to operate within the market in synchronicity with his own moral and ethical boundaries.[18]

The widespread influence of Hayekian thought stands as an integral part of the American legal-economic tradition. The Reagan administration prioritised market-oriented solutions in the interests of wealth bifurcation, entrenching an ideological reluctance of state interference.[19] Although subsequent regulation in other aspects of society ensued, neoliberal principles continue to inform those of cyberlibertarianism, providing the theoretical basis for Big Tech regulation in modernity.[20]

a) Voluntary Rules: Fair Information Practice Principles

The Fair Information Practice Principles (hereafter FIPs), a set of voluntary rules, gives rise to the current market-based system. Originating from the 'HEW Report',[21] the FIPs were conceived from the difficulty in legislating against the 'enormous number of institutions dealing with personal data'[22] that had a legitimate need to harvest data in order to facilitate business.[23] The FIPs are based on five foundational concepts, with the most significant being 'notice' and 'choice'. The notice requirement stipulates companies are required to provide 'clear and conspicuous'[24] notice of their information practices and further notice as to whether

[14] Securities and Exchange Commission, Google, Inc. S-1 Registration Statement (SEC Com No 7375, 2004) 27.
[15] Securities and Exchange Commission, Facebook, Inc. S-1 Registration Statement (SEC Com No 7370, 2012) 67.
[16] Friedrich Hayek, *The Road to Serfdom* (1st edn, Routledge Classics 2001).
[17] ibid.
[18] ibid 63.
[19] Birsen Filip, 'Polanyi and Hayek on Freedom, the State, and Economics' (2012) 41(4) International Journal of Political Economy 69, 70.
[20] Andrew D. Murray, 'Nodes and Gravity in Virtual Space' (2015) 5 Legisprudence 195, 22.
[21] U.S. Department of Health, Education & Welfare, 'Report of the Secretary's Advisory Committee on Automated Personal Data Systems' No. (OS) 73, 94.
[22] Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum, *Privacy, Big Data, and the Public Good* (1st edn, Cambridge University Press 2014) 7.
[23] Mary J. Culnan, 'Protecting Privacy Online: Is Self-Regulation Working?' (2000) 19(1) Journal of Public Policy and Marketing 20, 26.
[24] Federal Trade Commission, *Privacy Online: A Report to Congress* (1998) 7.

they disclose such information to third parties.[25] Viewed as such, the 'notice' element attempts to imbue a sense of fairness into corporation-consumer negotiations, providing the necessary information to empower the market actor in his decisional capacity. When providing 'choice', corporations must present consumers with the opportunity to accept or decline the provider's terms of service.[26] These voluntary rules and the resulting 'notice and choice' paradigm can be seen in the ubiquitous privacy policy, a mechanism utilised by Big Tech and other information intermediaries.

b) State and Federal Legislation

The FIPs are complemented by legislation enacted at a federal and state level.[27] In contrast to the EU's General Data Protection Regulation (hereafter GDPR),[28] the US is yet to enact an omnibus piece of privacy legislation and thus cannot enforce monolithic protection against Big Tech-related data harms. Sectoral privacy legislation exists within the public realm, exhibited by existence of the Fair Credit Reporting Act,[29] the Privacy Act,[30] the Health Insurance Portability and Accountability Act[31] and the Children's Online Privacy Protection Act.[32] However, the aforementioned legislation is not applicable to the private realm. Alternatively, enforcement measures against Big Tech are brought by the FTC, the de facto regulator of online privacy in the US. Powers to do so are conferred by the Federal Trade Commission Act,[33] permitting enforcement action on the basis of 'unfair or deceptive acts'.[34]

Federal adjudication is supplemented by state-level legislation. However, due to the disparate privacy-protecting cultures prevalent throughout the US, state-level protection often lacks force. Although the majority of states are yet to enact substantive legislation, Nevada, Maine and California have embarked on a regulatory upsurge,[35] with the latter effecting a Bill on 1st January, acknowledged as the most comprehensive state-level protection policy.[36] The

[25] ibid 15.
[26] ibid 16.
[27] Skeel, Jr. (n 13) 155.
[28] Council Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regards to the processing of personal data and on the movement of such data, and repealing Directive 95/46/EC OJ L119/1 (Hereafter GDPR Regulation).
[29] Fair Credit Reporting Act 1970.
[30] Privacy Act 1974.
[31] Health Insurance Portability and Accountability Act 1996.
[32] Children's Online Privacy Protection Act 1998.
[33] Federal Trade Commission Act 1914.
[34] ibid Section 5.
[35] Mitchell Noordyke, 'US State Comprehensive Privacy Law Comparison' (IAPP) <https://iapp.org/resources/article/state-comparison-table/#> accessed 19 December 2019.
[36] Data Guidance, 'Comparing Privacy Law: GDPR v. CCPA' (Future of Privacy Forum, December 2019) <https://fpf.org/2019/12/18/comparing-privacy-laws-gdpr-v-ccpa/> accessed 24 February 2020.

California Consumer Privacy Act (CCPA),[37] having been compared[38] to the GDPR,[39] provides for the 'right to be informed' of information being collected,[40] 'the right to request deletion of personal information',[41] 'the right to know whether personal information is being sold or disclosed'[42] and 'the right to opt out of the sale of personal information',[43] *inter alia*. Its limiting factor, however, is its territorial effect; the Act solely applies to Californian citizens. Due to California's size and influence in the techno-political arena, commentators have contemplated its potential to catalyse cultural change.[44] However, the Act does not actually curtail the data collection practices of the bound corporations; it simply requires them to engage in a more transparent dialogue with consumers, usually by means of a privacy notice. Due to the inefficiencies in the FIPs, to be discussed, this paper questions the efficacy of the notice, and therefore the protective force of the Act.

3. Evolution of Privacy and Privacy Protection

Due to the 'corporate mythology, opacity, complexity and size'[45] mutually exhibited in both Big Tech and Big Banks, financial regulation serves as the optimal regulatory foil. In both markets, corporate actors ostensibly prioritise risk-taking, straining the limits of corporate governance and consumer welfare in pursuance of profit maximisation.[46] The information asymmetry, as a hallmark of Wall Street subterfuge and deceit, was a weapon employed by Big Banks during the 2006 Subprime Mortgage Crisis,[47] allowing lenders to capitalise on homeowner ignorance and optimism. In an attempt to curb future predation, regulators played a 'cat-and-mouse game',[48] enacting subsequent legal guidelines in the Dodd-Frank Wall Street Reform and Consumer Protection Act,[49] which aimed at introducing greater protective mechanisms for consumers in financial dealings.

[37] California Consumer Privacy Act 2018.
[38] Data Guidance (n 36).
[39] GDPR (n 28).
[40] CCPA (n 37) Section 1798.100 b.
[41] ibid Section 1798.105 b.
[42] ibid Section 1798.115 a (2).
[43] ibid Section 1798.120 b.
[44] Jedidiah Bracy, 'With The CCPA Now In Effect, Will Other States Follow?' (IAPP, January 2020) <https://iapp.org/news/a/with-the-ccpa-now-in-effect-will-other-states-follow/> accessed 23 February 2020.
[45] Foroohar (n 1) 196.
[46] ibid 99.
[47] ibid 196.
[48] Skeel, Jr. (n 13) 158.
[49] Dodd-Frank Wall Street Reform and Consumer Protection Act 2010.

Privacy is in the midst of a similar crisis, evidenced by the 2016 Cambridge Analytica Scandal. The firm, lauded for its expertise in psychological warfare,[50] partnered with Facebook to leverage the information asymmetry exhibited throughout the platform, targeting 'persuadable' voters with propaganda pertaining to the Republican nominee for President, Donald Trump.[51] The event allegedly compromised the election process,[52] bringing contemporary understandings of democracy into sharp focus. It is questioned why the regulatory response, or lack thereof, diverges so greatly from its financial counterparts.

On assessment of the harm suffered by victims of Big Tech and Big Banks, this dichotomy is understandable, albeit not justifiable. Following the economic downturn of 2007, 8.8 million US citizens were made redundant,[53] catalysing mass foreclosure and poverty proliferation. Facebook users, however, experienced an intangible harm– their decisional autonomy was unwittingly relinquished, potentially undermining the foundational premise of democratic politics. The former is viewed as an overt injury, one that can be quantified evidentially and statistically. The latter harm, however, exhibits a shift to the metaphysical– victims were left unidentified and unheard, with many incognizant to the very existence of a violation. Consequently, privacy invasions are perhaps viewed as lesser within the US harm spectrum, explaining the reluctance of state intervention.

Since the prominence of informational privacy has come to light, the scholarship and judiciary have struggled to reconcile it with other norms.[54] The individualistic, atomised conception of privacy typically fails to triumph in the utilitarian balancing of interests. In such calculations, collective norms such as liberty and security acquire default primacy.[55] Consequently, the cultivated culture is one in which privacy is readily subjugated in the norm hierarchy.

In engaging in a comparative analysis between the US and the EU, diverging privacy attitudes are brought into sharp focus. In the US, privacy is not framed as a constitutional right, as held in *Katz v United States*.[56] The case established the seminal 'reasonable expectation of

[50] Alex Pasternack, Jesse Witt, 'Before Trump, Cambridge Analytica Quietly Developed Psy-ops For Militaries' (Fast Company, September 2019) <https://www fastcompany.com/90235437/before-trump-cambridge-analytica-parent-built-weapons-for-war> accessed 2 January 2020.
[51] Foroohar (n 1) 114.
[52] ibid.
[53] Christopher J. Goodman and Stephen M. Mance, 'Employment Loss and the 2007-09 Recession: An Overview' (2011) 134 Monthly Lab Rev 3.
[54] Pozen (n 2).
[55] ibid.
[56] *Katz v Unites States*, 389 U.S. 347 (1967).

privacy' test, extending the Fourth Amendment[57] prohibition of unlawful searches and seizures to areas the individual subjectively deems private.[58] The case advances the doctrine of unlawful encroachment of public entities, excluding private corporations from its ambit. This trend is exhibited throughout the American legal landscape–its founding document, the Constitution,[59] was enacted in defiance of unjust taxes and oversaturation of power, enshrining republicanism and liberty as civil essentialities.[60] Contrastingly, European conceptions of privacy are rooted in dignity, largely due to the 'reaction against fascism and especially against Nazism'.[61] The resulting rights-based protective doctrine, the European Convention on Human Rights,[62] has universal application, meaning the Article 8[63] and the Article 8 'Protection of Personal Data'[64] under the EU Charter of Fundamental Rights[65] apply to both private and public entities. By entrenching privacy protection within the Charter, European conceptions of privacy are rooted in respect and dignity for the person[66] in all social and commercial transactions.

The US liberty-based conception of privacy has prepared it as the prime conduit to facilitate other rights, catalysing constitutional change yet ironically denying it weight in itself. The epoch-making *Lawrence v Texas* established the 'right to privacy' when declaring the unconstitutionality of laws prohibiting homosexual relations between consenting adults.[67] However, the court, in its habitual manner, focused on the government transgression of personal privacy, with Justice Kennedy opining 'liberty protects the person from unwarranted government intrusions into a dwelling, or other private places'.[68] The concept was further employed in *Roe v Wade*, the seminal case which legalised access to abortions. It is clear from the aforementioned cases that conceptualising privacy in reductionist terms proves to be a significant barrier in privacy litigation.[69]

4. Privacy Violations in the 21st Century

[57] United States Constitution, Amendment IV.
[58] *Katz* (n 56).
[59] United States Constitution.
[60] William C. Heffernan, *Privacy and the American Constitution* (1st edn, Palgrave Macmillian 2016) 25.
[61] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale LJ 1151, 1165.
[62] European Convention on Human Rights.
[63] ibid Article 8.
[64] Charter of Fundamental Rights of the European Union.
[65] ibid Article 8.
[66] Whitman (n 61) 1160.
[67] *Lawrence v Texas*, 539 U.S 558 (2003).
[68] ibid (Justice Kennedy) 1.
[69] *Roe v Wade*, 410 U.S. 113 (1973).

For decades, privacy has been at the forefront of human interest, evidenced by the Orwellian presentation of invasive surveillance in the arts.[70] However, more recently, privacy concerns have moved from an abstract, foreign concern, to one that is pervasive throughout society. This section will discuss the impacts of violating consumer privacy, highlighting its requisite quality for human development. Such a discussion will serve to substantiate the importance of a robust, incorruptible, and privacy-centric regulatory system.

In relation to Big Tech, privacy violations occur in a number of ways. The FTC demonstrated that the non-disclosure of information and the failure to notify users of privacy-related changes constituted a breach,[71] as argued in *In re Facebook, Inc.*[72]. Breaches may also occur as a result of Big Tech's encroachment into other sectors, highlighted by concerns over Google's $2.1 billion acquisition of FitBit, wherein the tech giant gained access to data profiles of a particularly sensitive nature.[73]

Privacy invasions may occur subsequent to the data collection itself, with algorithmic treatment profiling consumers into intentionally undisclosed classifications. In a 2014 investigation, the FTC revealed some of the mysterious categories in which consumers are assigned: 'Cholesterol Focus', 'Diabetes Interest', 'Financially Challenged' and 'Urban Scramble'.[74] Zuboff, a prolific commentator on data aggregation, notes that through profiling, companies may 'nudge, tune, herd, manipulate, and modify behaviour in specific directions'.[75] This considered, breaches of privacy have the potential to go far beyond mere observance.

Imagination need not be stretched to appreciate the devastating impact of data aggregation. Altman and Westin have noted the self-evaluative quality to privacy which, if breached, results in 'stripping the individual naked of his human dignity by exposing his personal life to public scrutiny'.[76] Additionally, privacy invasions can influence 'psychological functioning, stable interpersonal relationships and personal development'.[77] Platforms such as Twitter and Facebook play a central role in persona creation and identity maintenance,[78]

[70] See: George Orwell, *Nineteen Eighty-Four*; Aldous Huxley, *Brave New World*.
[71] Asuncion Esteve, 'The Business of Personal Data: Google, Facebook, and Privacy Issues in the EU and the USA' (2017) 7(1) International Data Privacy Law 36, 42.
[72] *In re Facebook, Inc.*, C-4365, 2012 FTC LEXIS 135 (F.T.C. July 27, 2012) (Decision and Order).
[73] Isobel Asher Hamilton, 'Google's $2.1 billion Fitbit Acquisition Is A Major Privacy Risk, Europe Data Body Warns' (Business Insider, February 2020) <https://www.businessinsider.com/europe-google-fitbit-acquisition-privacy-risk-2020-2?r=US&IR=T> accessed 4 April 2020.
[74] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability*, (May 2014) V.
[75] Shoshana Zuboff, *The Age of Surveillance Capitalism* (1st edn, Profile Books 2019) 202.
[76] Katherine Glac, Dawn R. Elm, and Kirsten Martin, 'Areas of Privacy in Facebook: Expectations and Values' (2014) 33(1) Business and Professional Ethics Journal 147, 150.
[77] Stephen T. Margulis, 'Privacy As A Behavioural Concept' (2003) 59(2) Journal of Social Issues 243, 246.
[78] Glac (n 76) 150.

providing an optimal ecosystem to facilitate influence and manipulation. For example, leaked documents detail Facebook's role in tracking when teenagers feel 'insecure, worthless…[and] useless… and can micro-target ads' in response to this vulnerability.[79]

Online privacy also has links to the democratic arena, providing opportunities for political expression and deliberation.[80] However, genuine political participation presupposes insulation from observation and influence,[81] factors which are distinctly lacking in the online sphere due to data aggregation and profiling. Through the creation of echo chambers, behavioural preferences are analysed and projected back through advertisements, selective news reports and 'fake news'. Lessig reports 'the system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern'.[82] For this reason, namely the hindering of decisional autonomy and democracy, the current system's ability to truly liberate the individual in accordance with its ideological mandate is questioned.

5. Consumer Demand for Privacy: Addressing the Privacy Paradox

It is a staid truism that privacy is a subjective norm, as is the manner in which individuals prioritise privacy. In an empirical study exploring this subjectivity, Westin devised a scale in which individuals are classified, noting that the majority of individuals fell somewhere in between the categorisations.[83] Privacy fundamentalists epitomise those that reject the revocation, upholding privacy in its ability to foster autonomy and dignity. Privacy pragmatists encapsulate those who are preordained in relinquishing their privacy in return for specific goods, services, or other norms. As such, the market-based argument could be advanced on the basis that some consumers, the privacy pragmatists, don't seem to support regulation of Big Tech.[84]

The neoliberal attitudes of internet policy have been further shaped by this distinction and that of Paul Samuelson's 'Revealed Preferences' theory. The theory contends, on application to Big Tech, that data collection should reflect a consumer's actions, rather than their enunciated claims. It is irrelevant that 50% of users desire increased privacy protection

[79] Foroohar (n 1) 117.
[80] Paul M. Schwartz, 'Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practice' (2000) 2000 Wis L Rev 743, 734.
[81] ibid 761.
[82] ibid 747.
[83] Jennifer King, 'Taken Out of Context: Empirical Analysis of Westin's Privacy Scale' Symposium on Usable Privacy and Security, (Indiana 2014).
[84] Riley Griffin, 'Facebook Users Still Fear For Their Privacy' (Bloomberg, 5 September 2018) <https://www.bloomberg.com/news/articles/2018-09-05/facebook-users-still-fear-for-their-privacy> accessed October 2019.

on Facebook[85] as the platform hosts over 2 billion users. This behaviour is referred to as the 'Privacy Paradox'[86]– consumers claim to value privacy but continue to engage in detrimental activities. In fact, Mark Zuckerberg, founder of Facebook, has repeatedly de-prioritised privacy as part of his business model, stating 'privacy is no longer a social norm'.[87]

This paper challenges the legitimacy of the Paradox. Urban and Hoofnagle[88] refute the relevance of Westin's study to modern privacy concerns, persuasively observing that the notion of rational bargaining presupposes informed knowledge of data collection practices.[89] As will be discussed, this necessary knowledge is of disparate possession between the parties. As such, the verity of the paradox is undermined, bringing its weaponization in the market-based privacy agenda into question.

6. Conclusion

This section has explored the evolution of privacy-related norms, its culturally contingent nature and consumer demand for privacy in modernity. It has been argued that neoliberal ideals have formed the regulatory basis for many sectors including Big Tech. However, Big Tech is distinguishable from its financial counterparts in terms of the intangible harm it instigates. In disregarding these harms, notions such as democracy and equality are compromised, making US attitudes towards privacy increasingly problematic. The 'Privacy Paradox' was subsequently explored to exhibit how the market-based system, hinged on informed consent, is an unsuitable model for Big Tech regulation. Such a discussion is necessary to frame the context in which various data-related inadequacies have emerged; a focal point of the remainder of the paper.

C. AN EVALUATION OF THE SUFFICIENCY OF MARKET RULES AND ENFORCEMENT MECHANISMS

1. Introduction

This section will address the specific inadequacies of the current regulatory framework. Based on the aforementioned FIPs, the privacy policy claims to provide 'notice' of data collection

[85] Griffin (n 84).
[86] Hsuan-Ting Chen, 'Revisiting the Privacy Paradox on Social Media with an Extended Privacy Calculus Model' (2018) 62(1) American Behavioural Scientist 1392, 1412.
[87] Bobbie Johnson, 'Privacy is No Longer a Social Norm, Says Facebook Founder' *The Guardian,* (Las Vegas, 11 Jan 2010) < https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> accessed 10 November 2019.
[88] Chris J. Hoofnagle and Jennfer M. Urban, 'The Privacy Pragmatic as Privacy Vulnerable' (2014) UC Berkeley Public Law Research Paper No. 2514381 1, 1.
[89] ibid 3.

practices and a 'choice' to accept or decline. In analysing the content of the FIPs, the paper highlights their failure to protect consumers against the malicious practices of Big Tech. It will be argued that these inadequacies, coupled with the FTC's jurisdictional incompetency, form a regulatory framework that is wholly insufficient in upholding privacy. Analysis of the current system's shortcomings will later be used to bolster the argument that state-based regulation is preferable in the interests of robust rights protection.

2. Inadequacies of the Fair Information Practice Principles

The FIPs, when proposed, embodied five values[90] which were subsequently adopted and transformed into various frameworks. In the 1980s, the Organisation for Economic Co-operation and Development (hereafter OECD) recommended the adoption of six additional principles[91] in an attempt to engender substantive protection. In a 1998 advisory statement,[92] the FTC formally adopted only four principles in a report to Congress: Notice, Consent, Access, and Security.

One of the main criticisms of the FIPs is their antiquity. Developed during the 1970s and implemented throughout the 80s and 90s, the FIPs addressed data collection concerns such as the 'telephone tap, the wireless microphone [and] the automatic surveillance camera'.[93] Despite their open-textured nature, they serve to fit the information collection of a bygone era, in which transmission occurred on an infrequent basis. Hartzog comments on the FIPs redundancy with regards to their modern application, emphasising the 'near ubiquity' of Big Tech in the 21st century,[94] coupled with the contemporary use of algorithms and propensity for malicious data aggregation. For instance, analysis of mouse tremors and 'average scrolling velocity' has the ability to reveal the early onset of Parkinson's or Alzheimer's,[95] an action hardly feasible to the FIPs' creators.

The severable nature of the FIPs offers US entities the opportunity to adopt them on an ad-hoc basis and adapt them to their commercial needs.[96] Whilst the OECD adopted eight of the eleven principles, the Europeans placed all eleven principles on a statutory footing.[97] The FTC, however, adopted just four principles in their advisory document, omitting the OECD's

[90] Woodrow Hartzog, 'The Inadequate, Invaluable Fair Information Practices' (2017) 76 Md L Rev 952, 962.
[91] ibid.
[92] FTC Report (n 24) 7.
[93] U.S. Department of Health, Education & Welfare Report (n 21) 29.
[94] Hartzog (n 90) 953.
[95] Katharine Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (2019) University of New South Wales Research Paper 53/2019, 22 <http://www.austlii.edu.au/au/journals/UNSWLRS/2019/53.html> accessed 17 December 2019.
[96] Hartzog (n 90) 961.
[97] ibid 962.

Collection Limitation, Openness and Accountability principles, the very principles that provide substantive consumer protection. In opting for a purely procedural approach, the FTC has negated any opportunity for individual and collective redress, fostering 'suggestive rather than prescriptive'[98] guidelines, in which companies evade penalty unless a Section 5 claim is triggered, a situation discussed later in the paper. In essence, the FTC omissions permit Big Tech to operate with relative impunity. It is important to note that these are advisory guidelines, and do not bind relevant parties to ensure their delivery. As such, unless a corporation is particularly data-conscious, the FIPs represent the maximum threshold of protection, with many corporations utilising their autonomous power within the market-based system to determine the scope of the 'notice' and 'choice', subsequently falling far below the FTC standard.

3. Insufficiencies with the 'Notice and Choice' Model and Privacy Policies

Using the 'notice and choice' paradigm, Big Tech claim to enforce data protection through privacy policies. Their notion of privacy protection is hinged on the concept of consumer control, or rather privacy self-management, a tenet paradigmatic to the privacy private order. However, as will be discussed, the privacy policy serves to impair its own legitimacy due to its unilateral reach and inability to deliver information accurately. This criticism serves as yet another attack on market-oriented solutions regulating the data economy.

a) 'Notice' is Ambiguous

The open-textured nature of the FIPs feeds directly into the privacy policy, allowing corporate actors to utilise the flexibility to their commercial advantage. The FTC, when adopting the principles, admonished granularity in this area of the law, stating regulation should be 'phrased in general terms and be technologically neutral'.[99] Market-based advocates support this claim, praising the enabling power of the FIPs in their ability to adapt to the rapidly advancing technological scene.[100]

Many corporations, *prima facie*, fulfil the notice requirement through the existence of the policy, often disclosing that data harvested may be shared with 'third parties'.[101] It has been

[98] FTC Report (n 24) 10.
[99] ibid iii.
[100] Milken Institute, 'FinTech: Who Regulates It and Why It Matters' (2016) <https://milkeninstitute.org/sites/default/files/reports-pdf/FinTech-Who-Regulates-It-and-Why-It-Matters2.pdf> accessed 4 December 2019.
[101] Amazon Services, 'Amazon Privacy Notice' (January 2020) <https://www.amazon.com/gp/help/customer/display.html?nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_FE2374D302994717AB1A8CE585E7E8BE> accessed 28 April 2020.

noted that only 7% of firms define who these affiliates are,[102] nor do they specify their motivation for the transfer. Specification is not explicitly required by the FIPs themselves, but 'clear and conspicuous' notice is necessary. Lacking clarification of what this entails, Big Tech may evade the requirement of meaningful notice on a technicality, releasing private consumer data to a wealth of unrelated entities.[103]

b) 'Notice' is Confusing

In granting notice to their users, corporations rely on convoluted policies[104] in an attempt to discombobulate rather than inform. Corporations are renowned for burying vital information in the midst of both vague and overwhelmingly technical language, utilising opacity as a vehicle for concealed data practices.[105] The FTC has openly condemned such manipulation in a Preliminary Report to Congress, stating that the 'notice and choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand'.[106] It is this strange presentation of ambiguous language, simultaneously fraught with legal minutiae, that obfuscates to the point of redundancy.

On consultation of empirical evidence, the unworkability of the current mechanism comes into sharp focus. The average policy is 2,227 words long, requiring 201 hours of annual reading[107] for the number of privacy policies accessed by the average user. Aside from being a considerable inconvenience in a convenience-driven society, Martin suggests the protracted length imbibes a misplaced trust in the consumer, in that it presents a Tabula Rasa.[108] Exploring the cognitive dissonance between actual and perceived privacy, she suggests that the incessant onslaught of supposed privacy-protecting mechanisms is likely to quell privacy concerns, enforcing a false reality.[109] The onus is placed on the consumer to educate themselves to an unreasonable degree on data collection processes, but to simultaneously question perceived notions of privacy presented as a Tabula Rasa. With this act being recognised as a virtual impossibility, the asymmetry between the actors escalates. The issue is further exacerbated by the oligopolistic nature of the market. Due to Big Tech's commercial prowess and competitive

[102] Florencia Marotta-Wurgler, 'Understanding Privacy Policies: Content, Self-Regulation and Market Forces' (2015) NYU Law and Economics Research Paper No.16-18) 6 < https://www.law.uchicago.edu/files/file/marotta-wurgler_understanding_privacy_policies.pdf> accessed 11 November 2019.
[103] Foroohar (n 1) 238.
[104] Amazon Services (n 101).
[105] Hartzog (n 90).
[106] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (2012) 1, 2.
[107] Marotta-Wurgler (n 102) 6.
[108] Kirsten Martin, 'Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online' (2015) 34(2) Journal of Public Policy & Marketing 210, 227.
[109] ibid 220.

position bolstered by network effects,[110] consumers have no choice but to assume the subjugated position.

c) 'Choice' is Redundant

The element of 'choice' in the privacy policy is central to its workability. The choice empowers users who operate within the free market, allowing them to ascertain their own moral and ethical boundaries. When making the decision to accept a company's notice, the consumer is presented a decision: Accept or Decline. However, such a choice is problematic in that it is illusory;[111] rather consent is a condition of service,[112] and the unilateral imposition of terms is camouflaged under alleged voluntarism.

In coining the type of transaction 'Boilerplate', Radin explores disparity in bargaining power between the parties[113]–'[a]greement has become a talismanic word merely indicating that the firm deploying the boilerplate wants the recipient to be bound'.[114] Unilateral terms grant the technological firm significant bargaining power, introducing a distinct hierarchy within the private order. Furthermore, by declining the terms of the offer, thus opting out of the services provided by Big Tech, consumers risk social isolation and relinquish participation in the contemporary information society. Papacharissi and Gibson encapsulate this sentiment, remarking 'byte by byte, our personal information is exchanged as currency to gain digital access to our own friends'.[115]

Additionally, the content of the policy itself may preclude meaningful choice. The vast majority of policies stipulate that data may be transferred to 'third parties' or 'affiliates'. Third parties are rarely subject to the binding force of the policy,[116] meaning that once authorised, the transaction removes any opportunity for continued control over data profiles. In reaping the benefits of connectivity provided by Big Tech, the user is associated with a number of unknown entities, therefore eroding the distinctly libertarian quality of the data economy.

d) 'Choice' is Paradoxical

---

[110] Foroohar (n 1) 129.
[111] Neil M. Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stanford Tech L Rev 431, 444.
[112] Fred H. Cate, 'The Failure of Fair Information Practice Principles' (2006) *Consumer Protection in the Age of the Information Economy* 343, 358.
[113] Margaret Jane Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (1st edn, Princeton University Press 2013).
[114] ibid 14.
[115] Leonard Reinecke and Sabine Trepte, *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (1st edn, Springer 2011) 84.
[116] Nestor Duch-Brown, Bertin Martens, Frank Mueller-Langer, 'The Economics of Ownership, Access and Trade in Digital Data' (2017) JRC Digital Economy Working Paper 1/2017, 15 <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf> accessed 24 March 2020.

The final issue with regard to 'choice' is its paradoxical nature–decisional autonomy does not scale.[117] This may seem surprising when considered in the context of the market-based system with prominent proponents such as Sen prioritising negative liberty,[118] as it would be assumed that choice proliferation grants great opportunity to advance negative liberty. Rather, the opposite is true. Schwartz has explored this phenomenon extensively in his seminal work, *The Paradox of Choice.*[119] He postulates '[a]s the number of choices grows further, the negative escalates until we become overloaded. At this point, choice no longer liberates, but it debilitates.'[120] The choice granted to us is 'overwhelming to the point of futility'.[121]

In relation to privacy, consumers are subject to a constant barrage of alleged 'choices' which must be fulfilled to participate in the tech-focused society. In oversaturating the consumer with perplexing decisions, the efficacy of the self-regulatory approach is undercut as it denies the market actor the ability to comprehend the panoply of information, further challenging the market-based system's ability to protect consumer privacy.

4. The FTC's Jurisdictional Incompetency

The FTC itself is a barrier to consumer privacy. It cannot be denied that the agency possesses adjudicative capabilities, but the scope and force of these powers are disputed. In its absence, the corporation assumes the role of the regulator, affording themselves significant discretion in the creation of rules and avoidance of substantial penalty.

As previously mentioned, privacy violation claims fall within the ambit of Section 5 of the Federal Trade Commission Act, which stipulates that '[u]nfair or deceptive acts or practices in or affecting commerce are hereby declared unlawful'.[122] It has been observed that the FTC rarely declares actions 'unfair', habitually opting to bring proceedings under the 'deceptive' prong of Section 5.[123] In doing so, the agency has significantly narrowed its own scope to penalise commercial entities, thus reducing its capacity to enforce meaningful and substantive norms. Furthermore, the 'deceptive' prong of the provision is yet to be defined by the FTC, perhaps mirroring its position towards the FIPs in prioritising flexibility. By quoting Baum and Baker, the overarching notion of malleability is reiterated–'[Section 5] cannot be defined in terms of constants. More broadly, it is a recognition of an ever-evolving commercial dexterity

[117] Hartzog (n 90) 956.
[118] Amartya Sen, 'Markets and Freedoms: Achievements and Limitations of the Market Mechanism in Promoting Individual Freedoms', (1993) *Oxford Economic Papers*, 45(4) 519, 525.
[119] Barry Schwartz, *The Paradox of Choice: Why More is Less* (1st edn, Harper Perennial 2004).
[120] ibid 2.
[121] ibid 64.
[122] Federal Trade Commission Act 1914 (n 33) Section 5.
[123] ibid.

and the personal impact of economic power as important dimensions of trade'.[124] This quote considered, it is evident that Section 5 is commerce-oriented, consequently favouring the former notion in the balancing act between commercial interests and personal privacy.

The FTC's reluctance to accept a holistic conception of privacy is exacerbated by exogenous limits on its jurisdictional competency. When the FTC reasonably believes a corporate action falls under the umbrella of Section 5,[125] it cannot, *prima facie*, issue a financial penalty–it may only issue a complaint in the form of a consent decree, a conclusion reached between a defendant and the court, but liability is not assumed. The court simply identifies the issues and provides guidance for future action. Although the defendant isn't permitted to assume liability, the agreement does carry proactive legal force, meaning that any future breach of the agreement would be subject to penalty. The inability to issue an initial penalty brings the sanctioning capability of the decree into consideration, as '[c]onsent decrees reveal primarily how hard the axe has fallen and not where it will hit next'.[126]

In considering the consent decree issued to Facebook in 2012, and its subsequent breach of the order in 2019, one can fully appreciate the practical redundancy of this process. The 2012 issue related to Facebook's deceptive privacy settings and the dissemination of information with advertisers. With regards to the first issue, Facebook made private user information available to Applications their Friends had used,[127] following which the FTC held that 'the representation set forth… constitutes a false or misleading representation'.[128] Similarly, the FTC noted that sharing user information to advertisers contravened the agency's interpretation of Facebook's privacy policy–'Facebook has represented, expressly or by implication, that Facebook does not provide advertisers with information about its users'.[129] Such contravention, according to the FTC, also constituted a 'false or misleading representation'.[130] The consent decree subsequently ordered a series of legal restrictions on Facebook's operations, merely prohibiting further misrepresentation.

In response to the 2019 breach, the FTC noted that despite making small changes to privacy settings, the changes failed to inform users that their information was available to 'more

[124] Eugene R. Baker and Daniel J. Baum, 'Section 5 of the Federal Trade Commission Act: A Continuing Process of Redefinition' (1962) 7 Vill L Rev 517, 519.
[125] Federal Trade Commission Act 1914 (n 33) Section 5.
[126] Subcomittee Number 5, *Consent Decree Program of the Department of Justice*: Volume 3, Part 2, (American Telephone and Telegraph Co, 1958) 4082.
[127] *In re Facebook, Inc.* (n 72).
[128] ibid para 18.
[129] ibid para 41.
[130] ibid para 42.

than one million third-party developers whose apps could be used by their Friends'.[131] In lieu of taking the case to trial, the FTC reached a settlement of $5 billion, and a proposed order which releases Facebook from all previous Section 5 claims.[132] The proposed order notes that if a new product or service poses a 'material risk' to user privacy, the company must prepare a Privacy Review Statement. Commissioner Rohit Chopra dissented to the proposed order, noting that '[the order] does not require users to consent to the integration; it requires only that Facebook describe its consent procedures'.[133] The decision to release Facebook from all previous Section 5 claims and order violations is similarly problematic. Reducing a breach of data to a negotiation, in which previously alleged liability can be wiped, means true accountability cannot be achieved.

The FTC's internal culture not only ignites current privacy concerns but could harm prospective regulation. Cortez argues that current underenforcement may impact future laws, noting it can 'calcify, creating a weak default position that leads to suboptimal regulation over longer periods'.[134] In amassing huge wealth, fiscal forfeit represents a minimalist reprimand in the context of Big Tech's total revenue. When fined $5 billion, assertions of the 'historic' and 'ground-breaking' nature[135] of the sanction were rife. However, the supposed 'historic' settlement only made up one quarter of Facebook's annual profits, and one month of annual revenue.[136] The deterrent force of the sanction is therefore questioned. Information intermediaries, with knowledge of the forgiving sanction hierarchy, have little incentive to abide by the FTC's requirements and may continue to violate their policies in a recidivist manner.

5. Conclusion

This section has explored the internalities of the market-based system, namely the 'notice and choice' model and the resulting privacy policy. It has been concluded the consumer's ability to receive true 'notice' and 'choice' is significantly hindered by the procedural adoption of rules. As such, the market-based system fails in its goal of liberating the consumer. Furthermore, the pro-settlement culture within the FTC enables Big Tech in its privacy-invasion capacity, therefore providing breach victims little opportunity for redress. Such a discussion has the

[131] *United States of America v Facebook, Inc* (2019), Case No. 19-cv-2184 87.
[132] ibid (Dissenting Statement from Commissioner Rohit Chopra).
[133] ibid 13.
[134] Nathan Cortez, 'Regulating Disruptive Innovation' (2014) 29 Berkeley Tech LJ 175, 227.
[135] Nilay Patel, 'Facebook's $5 billion FTC Fine Is An Embarrassing Joke' (The Verge, July 2019) <https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke> accessed 24 November 2019.
[136] ibid.

purpose of further substantiating the argument that the market-based system is a wholly unsuitable model for privacy protection.

D. A GENERAL CRITIQUE OF THE MARKET-BASED SYSTEM AND AN ASSESMENT OF THE SUITABILITY OF STATE-BASED REGULATION

1. Introduction

The individual facets forming the market-based system have been analysed and declared insufficient for their purpose. The discussion thus far shall be used as a foundation to further the more general argument that market-based regulation is unsatisfactory. In drawing upon legal, economic, and ethics-based commentary, arguments for self-regulation shall be explored, namely the proliferation of innovation, avoidance of legal fragmentation and the autonomy of the individual. The normative case for state-based regulation will then be investigated. The paper's previous discussion on the inadequacies of the privacy policy and the resulting asymmetry will be used to reveal a self-regulatory system fraught with market failure, therefore negating the market's functioning in accordance with economic principles. The paper's argument relating to the FTC's jurisdictional incompetency will be employed to highlight a distinct lack of corporate accountability for privacy violations. The section concludes by building on previous discussions pertaining to the centrality of privacy to the human condition, arguing that unfettered data extraction and aggregation is both exploitative and dehumanising, therefore justifying the imposition of 'hard' legal rules and principles.

2. The Case for Market-based Regulation

a) The Encouragement of Innovation and Wealth Generation

The case for market-based regulation is intrinsically linked to the widely accepted corporate objective, wealth maximisation. Relating to the fictitious quality of the notional entity, Friedman infamously postulated that the only 'social responsibility of business… [is] to increase profits'.[137] In prioritising unfettered innovation, Big Tech forges a system affording itself optimal creative autonomy, utilising consumer data to build revolutionary infrastructures. As a corollary of innovation, wealth generation ensues, therefore it is the corporate prerogative to achieve this objective through whatever means necessary.

Market-based advocates note that the collectivist state is unable to navigate the maelstrom of the market. To govern a rapidly evolving industry, the reflective law would require drafting in an intricate and constant manner. Hayek admonished the state's ability to

[137] Milton Friedman, *Capitalism and Freedom* (3rd edn, University of Chicago Press 2002) 133.

legislate in these circumstances and elaborated on the hubris of the state–'freedom… depends on the circumstances of time and place, because only the individuals know the time and place'.[138] Market rules, absent a binding force, can be readily adopted, adapted, or ignored, and are thus reconcilable with technological ideals.

Big Tech's capability to violate privacy is a direct result of lexical ordering. Privacy protection and profit-maximisation exist in separate lexical orders, meaning the former need not be satisfied to achieve the latter.[139] This notion is central to Big Tech's success–it authorises exploitation of an endless resource pool afforded by diminished consumer protection, therefore evading the traditional challenges of supply chains and mass production. Stifling access to this resource through statutory regulation could ossify innovation, decreasing investor desirability and subsequent economic bifurcation.

Finally, one cannot overstate the symbolic power of stifling growth. Silicon Valley stands as the ultimate incubator for technological progression and is somewhat paradigmatic of the primordial American Dream–unencumbered growth, success, and economic maximisation. Specifically, the distinctly cyberlibertarian 'Californian Ideology'[140] as part of the modern American Dream envisions a Jeffersonian democracy, in which the democratisation of information offers the individual status as the guardian of his own destiny.[141] However, it is highly ironic that the free distribution of cyber-information fails to extend to the very information contained within the ubiquitous privacy policy.

b) Avoidance of Inappropriate Statutes and Legal Fragmentation

When regulating complex, divisive areas such as technology, the risk of enacting an unsuitable statute is significant. The federal and state-level legislative system, according to the market-based advocate, does little to account for subject heterogeneity and conduct diversity, generating problems pertaining to legal fragmentation and market distortion.

For example, states enacting privacy-protecting legislation may emulate California by prioritising stringent territorial regulation. However, this strategy will only succeed on universal and consistent application across the states. A Milken Institute report[142] explored states' cultural attitudes towards technology, and the subsequent disparities that flow from such

[138] Hayek (n 16) 79.
[139] Ian Ayres and John Braithwaite, *Responsive Regulation* (1st edn, OUP 1992) 27.
[140] Richard Barbrook and Andy Cameron, 'The Californian Ideology' (1996) 6(1) Science as Culture 44, 55.
[141] ibid.
[142] Milken Institute, 'State Technology and Science Index; Sustaining America's Innovation Economy' (2019) 17 <https://milkeninstitute.org/sites/default/files/reports-pdf/State-Tech-2018-FINAL%20%281%29.pdf> accessed December 2019.

findings. The Institute granted each state a score relative to their 'innovative pipeline'[143] and technology-related economic development. The lowest ranking state, Mississippi, gained a score of 19.78 on the State Tech and Science Index, whilst Massachusetts scored 86.25.[144] In previously discussing the diverging European and US attitudes to privacy protection, it was deduced that these attitudes are culturally contingent. There is nothing to say that this won't have the same effect in an intra-American context, with Massachusetts and Mississippi enacting entirely incongruous legislation. The disparity may exacerbate concerns pertaining to a 'race-to-the-bottom', in which certain states deregulate under their own sovereign discretion in an attempt to attract technological business and prosperity. Such inter-state jurisdictional conflicts may create legal voids, in which individual rights and liberties fail to receive protection on a statutory level. In response to these potential issues, market libertarians propose the market as a mechanism to avoid state-imposed regulatory gaps, as actors experience protection or liberation in accordance with his individual moral and ethical desires. Due to market-based issues explored in the second section, this paper rebuts the ability of the market actor to do so.

Pro-regulation advocates have responded to the issues associated with state regulation, suggesting the imposition of a universal legal order.[145] Federal legislation is particularly suited to privacy protection due to the innate trans-state mobility of data. This informed the European Union's decision to enact the GDPR,[146] its purpose being to 'do away with the current fragmentation in different national systems and unnecessary administrative burdens'.[147] However, the US is characterised by a high degree of cultural heterogeneity and political bipartisanship, and the disparity between the states with regards to their technological inclinations is not negligible. As such, a one-size-fits-all approach may not be suitable.

Furthermore, a uniform statute, in this context, is sure to have non-uniform application. Knight notes the potential for market distortion in enacting federal legislation; it '[prevents companies] from entering states whose smaller markets do not justify the additional regulatory burden'.[148] Moreover, a universal statute naturally assumes a monolithic business model which, in the corporate reality, is not the case. Smaller businesses bear the brunt of the

[143] ibid 1.
[144] ibid 2.
[145] Milken Institute (n 100) 17.
[146] GDPR (n 28).
[147] 'GDPR Compliance' (2018) 1(1) European Cooperation
< https://european-cooperation.eu/index.php/EC/GDPR_Compliance> accessed 23 February 2020.
[148] Milken Institute (n 100) 14.

regulatory burden due to their inability to meet compliance costs, therefore hindering their ability to operate within the market.[149] Big Tech, conversely, can leverage their ability to assume increased regulatory costs, further capitalising on their competitors' struggles. Big Tech has a history of acquiring start-ups and established firms, exemplified by Google's acquisition of 120 companies.[150] Faced with compliance issues, smaller companies have no choice but to acquiesce to the desires of tech giants, resulting in increased acquisition activity which decreases competition and increases Big Tech's market power. As such, regulating creates a judicial hydra, fuelling the power regulators attempt to curtail.

c) A Free Market Guarantees Autonomy of the Individual

Market-based regulation advocates bolster their argument by acknowledging fragmentation on a micro-level. Market liberalism, as inferred by its moniker, purports to emancipate the market from external forces. As an actor of the market, the individual is similarly emancipated and is free to invoke his individual morals relating to the use of his private property. This notion rests on the rejection of an objective ethical code, instead recognising the 'individual as the ultimate judge of his own ends'.[151] This neoliberal dialogue therefore upholds negative liberty,[152] or freedom from coercion.

It can be argued that this notion accommodates the wide variety of market actors identified by Westin, from fundamentalists to pragmatists. It is indeed a persuasive point that regulation should reflect the diversity amongst both consumers and business models; privacy pragmatists can freely engage with information intermediaries whilst privacy fundamentalists may invoke stringent moral limits on how to operate in the marketplace.

Nevertheless, this paper questions how this concept of 'negotiation' and 'bargaining' manifests in practice. With the information asymmetry commonly invoked by Big Tech, the extent to which individuals are truly autonomous is doubted. Ward suggests that, in the data transaction, consumers utilise a system rooted in Kantian ethics, proposing the categorical imperative as a check on their online conduct within the free market.[153] This moral framework suggests that individuals 'universalise' an action to determine whether the result restricts an individual in their autonomous capacity.[154] In applying such a framework to the Cambridge

[149] ibid.
[150] Foroohar (n 1) 105.
[151] Hayek (n 16) 60.
[152] Filip (n 19) 72.
[153] Ken Ward, 'Social Networks, the 2016 US Presidential Election, and Kantian Ethics: Applying the Categorical Imperative to Cambridge Analytica's Behavioural Microtargeting' (2018) 33(3) Journal of Media Ethics 133, 148.
[154] ibid 137.

Analytica Scandal and 'universalising' their microtargeting operation, Ward posits that the result undermines individual autonomy to a degree that engagement with such a company is 'ethically unjustifiable'.[155] To adequately disengage with the company, individuals should provide platforms with false information 'to disrupt accurate profiling' or abstain from platform use altogether.[156] However, by eliminating our digital footprint, the ability to partake in contemporary life is eroded. These emancipatory activities inadvertently undermine the autonomy of the individual, the very quality the market purports to protect.

This paper submits that, in lieu of Ward's futile moral skeleton, a robust legal framework is required. Similar to the quintessential libertarian, he romanticises the market, overstating the individual's capabilities in negotiating with information intermediaries. This raises a critique of free markets in general–they bear no resemblance to reality. The market-based data economy places the impetus on the consumer to an unconscionable degree. When coupled with rampant corporate mystification and manipulation, privacy self-management is a virtual impossibility.

3. The Case for State-based Regulation

a) Market Limitations Undermine the Functioning of the Free Market

An efficient market presupposes the absence of market failures, or 'the malfunctioning of the market because of imperfections in it'.[157] This paper contends that the data economy is fraught with market failures, making the market-based system a wholly inappropriate forum for privacy regulation. As such, state-based regulation is endorsed in order to rectify the market failures.[158]

Hayek and his contemporaries hailed private property rights as imperative to the private order, branding them 'the most important guarantee of freedom'.[159] In reality, the court has refuted the assumption that data has any intrinsic economic worth, bringing the proprietary question into light. In *Re JetBlue Airways Corporation Privacy Litigation,*[160] there was 'no support for the proposition that the personal information of an individual JetBlue passenger had any value'.[161] Likewise, in *Low v LinkedIn Corporation,*[162] the plaintiffs argued for a contractual reading of LinkedIn's privacy policy, alleging economic loss when the company

[155] ibid 137.
[156] ibid 143.
[157] Donald Rutherford, *Routledge Dictionary of Economics* (3rd edn, Routledge 2000).
[158] Duch-Brown (n 116).
[159] Hayek (n 16) 108.
[160] *In Re JetBlue Airways Corp. Privacy Litigation*, 379 F.Supp.2d 299 (E.D.N.Y. 2005).
[161] ibid 327.
[162] *Low v LinkedIn Corp*, 900 F.Supp.2d 1010 (N.D. Cal. 2012).

supposedly breached their guarantee of prohibiting third-party data transfers.[163] The court failed to recognise such a value from the aggregated data, stating that the plaintiff's theory is 'unsupported by decisions of other district courts'.[164]

The privacy policy, in stipulating its affiliation with third parties further precludes proprietary ownership of data profiles. The condition ensures the non-excludability of data,[165] fashioning it a non-rival good; intermediaries can reap its benefits due to its susceptibility to replication and mobility.[166] In granting availability to a wealth of unnamed parties, asserting property rights becomes a virtual impossibility. This market failure could be rectified by subjecting all third parties to the privacy policy, binding them by its terms and requiring the user to consent to individual data transfers. However, in navigating a complex network of contracts, the consumer is faced with a great inconvenience. Additionally, this suggestion has the potential to distort markets. If third party access is denied, the benefit from multi-party data aggregation cannot be realised, stifling downstream innovation.[167] In both granting and withholding property rights, suboptimal market outcomes are the result. As such, the paper rebuts the suitability of the market-based system regulating data collection.

A further archetypal market failure is the information asymmetry, induced by the shortcomings of the privacy policy. Due to the composition of the privacy policy and the excessive burden placed on consumers to interpret the document, any effort to rectify the asymmetry is rendered futile. Friedman elaborated on the asymmetry, noting that market transactions must be 'bi-laterally voluntary and informed'.[168] It is submitted that, due to the ambiguous and discombobulating nature of the FIPs and the privacy policy, the transaction fails to be informed, thus undermining the efficacy of the market-based system.

Not only does the manipulation of human behaviour constitute an economic limit in the market, it introduces a moral limit. It is contended that certain 'commodities', such as personal privacy, should not be for sale.[169] The thesis of Satz shall be invoked, who explores 'noxious' markets in their ability to engender vulnerability and compromise agency.[170] Satz orients her argument around organ sales and the sexual economy,[171] with justifications against sales rooted

[163] ibid.
[164] ibid 1028.
[165] Duch-Brown (n 116) 15.
[166] ibid 12.
[167] ibid 19.
[168] Debra Satz, 'The Moral Limits of Markets: The Case of Human Kidneys' (2008) 108 Proceedings of the Aristotelian Society 269, 274.
[169] Adam Moore, 'Privacy, Interests and Inalienable Rights' (2018) 5(2) Moral Philosophy and Politics 327, 355.
[170] ibid 349.
[171] Satz (n 168) 269.

in human dignity and ethics–the creation of an organ market places a value on the human condition, a price that inevitably differs between individuals on the basis of quality or health. In paraphrasing Dworkin, Satz comments on the benefit of drawing a 'prophylactic line'[172] around the body, preventing violation and nefarious manipulation of its components. Moore notes similar outcomes in the data economy.[173] Behavioural microtargeting, a practice commonly employed by information intermediaries, has the potential to undermine agency, precluding individuals from autonomous choice. Captological studies[174] have revealed that behavioural microtargeting undermines equal citizenship,[175] grouping consumers into subsets, a practice which inadvertently favours certain ideals over others.[176] Thus, in the interest of higher principles such as democracy and freedom of expression, state intervention, despite its paternalistic nature, is imperative to prevent further manipulation and malevolence.

b) State-based Regulation Ensures Accountability

This paper submits that state regulation is desirable in the interests of accountability. Within the market-based system, corporations are primarily accountable to each other. However, as discussed, Big Tech rests on a distinctly capitalist foundation, in which economic bifurcation is representative of a firm's supremacy. The separate lexical ordering of profit and protection results in a system where dominant players will continue to reduce privacy protection in a regulatory race-to-the-bottom.

Big Tech's avoidance of accountability is allegedly justified by the privatised nature of the firm. As it lacks a public dimension, its objective is not to serve society, but only those with a stake in the company, the shareholders.[177] However, this statement fails to recognise the quasi-state function of Big Tech. Sternberg's account of the corporation, which aligns with the privatised view, shall be expounded and rebutted on application to the Big Tech model.[178]

Sternberg distinguishes between the state and the corporation on the basis that the former has the ability to coerce subjects, a weapon lacking in the private company.[179] This notion is refuted on analysis of the Cambridge Analytica Scandal, in which the dark underbelly

[172] ibid 277.
[173] Moore (n 169).
[174] Foroohar (n 1) 111.
[175] Moore (n 169) 348.
[176] Blayne Haggart, 'The Government's Role in Constructing the Data Driven Economy' (Centre for International Governance Innovation, 5 March 2018) <https://www.cigionline.org/articles/governments-role-constructing-data-driven-economy> accessed 4 November 2019.
[177] Elaine Sternberg, *Corporate Governance: Accountability in the Marketplace*, (2nd edn, IEA, 2004) 33.
[178] ibid.
[179] ibid 142.

of persuasive technology[180] came to light. Facebook users were targeted with 'fake news' and passion-igniting images, with the intention being political coercion and manipulation relating to the 2016 US presidential election. It is submitted that the encroaching on the distinctly public realm of politics sufficiently refutes Sternberg's account of the corporation. In response, the FTC fined Facebook Inc. $5 billion dollars, the largest fine administered by the FTC in history.[181] Notably, those affected by the crisis received no remuneration for the violation, highlighting the FTC's inability to command substantive accountability. Belli comments on the constitutional significance of the incident, commenting that, due to the lack of transparency and accountability in the adjudication-settlement process, the constitutional right to due process is violated, in that it 'create[s] an excessive burden'[182] or barrier to access to justice.

Sternberg also claims that corporations lack the monopolistic quality of states.[183] This is readily refuted on simple analysis of the market. Facebook and Google assume 84 percent control of digital advertising,[184] whilst Google alone has an 88 percent share in the search engine market.[185] Due to the near certainty of the Big Tech monopoly, it is difficult to uphold Sternberg's non-accountability argument.

Diverging from Sternberg's analysis, Big Tech's quasi-state function is demonstrated by its civic and governmental power. It is a truism to say that the platforms provided by Big Tech permeate every corner of 21st century life. Platforms have become forums for democratic expression, with 62% of the US population accessing news outlets on social media, and President Trump exploiting Twitter as his primary vessel for political pronouncement.[186]

Big Tech assumes a state-like function by encroaching on the branches of government. In a legislative sense, Big Tech's dominant position within the free market affords them the position of rule drafter–the rules which they deem beneficial are authoritative. Furthermore, information intermediaries influence the creation of social rules. Rodrigues invokes Lessig's powerful assertion that 'code is law', contending that 'the individuals responsible for engineering the code are those who decide what can and cannot be done–our liberties'.[187] In

[180] Foroohar (n 1).
[181] *In re Facebook Inc.* (n 72) (Dissenting Statement from Commissioner Rohit Chopra).
[182] Luca Belli and Jamila Venturini, 'Private Ordering and The Rise of Terms of Service as Cyber-regulation' (2016) 5(4) Internet Policy Review 1, 10.
[183] Sternberg (n 177)142.
[184] Foroohar (n 1) 187.
[185] ibid 136.
[186] Brian L. Ott, 'The Age of Twitter: Donald J. Trump and the Politics of Debasement' (2017) 34(1) Critical Studies in Media Communication 59, 65.
[187] Clara Alves Rodrigues, 'Digital Gangsters: Are Facebook and Google a Challenge to Democracy' (2019) 11(3) Amsterdam Law Forum 30, 36.

considering the reductionist theory of technological determinism, the problem seems to be further exacerbated. Mumford issued a scathing critique of the societal role of technological determinism, postulating that the nefarious aim of such technologies 'is to displace life, or rather, to transfer the attributes of life to the machine and the mechanical collective'.[188] Those who drive social change are insulated from accountability, whilst their internal partialities and epistemological biases encroach on our democratic processes.

The issue is exacerbated by the executive quality of Big Tech's governance. Not only do firms draft and enforce rules governing the boundaries of society, they determine the nature of conduct permissible within those boundaries. The growing awareness of behavioural microtargeting has called commentators to elaborate on the emergence of the 'surveillance state'.[189] Throughout her work, Zuboff focuses on the resulting Hawthorne Effect, in which consumers refrain from the expression of potentially unpopular opinions.[190] Big Tech's potential to influence individual expressional autonomy has made the question of accountability all the more poignant.

Eels' account of 'industrial absolutism'[191] seems to relate to the contemporary situation. With the concentration of quasi-state power, Montesquieu's doctrine of the separation of powers[192] and resulting principles of legality are violated. The system largely falls outside the 'checks and balances' imperative to other collectives holding such power and influence. Operating in a public capacity, it seems illegitimate that such entities would be subject to private governance.

It is submitted that statutory regulation is the optimal choice to ensure accountability, however regulation can take many forms, with contract law and constitutional law providing the most popular options. This paper contends that a distinct shift in governance culture is required, endorsing the Privacy-as-Trust model[193] to introduce a fiduciary-type position for Big Tech in the data economy. Under the model, corporations are subject to the traditional principles of trusts law, in particular, the duty of care and the duty of loyalty. These principles

[188]Kevin Robins and Frank Webster, *Times of The Technoculture: From the Information Society to the Virtual Life* (Routledge 1999) 167.
[189] Zuboff (n 75).
[190] ibid.
[191] Ayres and Braithwaite (n 139) 124.
[192] Charles Baron de Montesquieu, *The Spirit of Laws* (1st edn, Cosimo Classics 2011).
[193] Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* (CUP 2018) 77.

are decidedly austere; the trustee must handle the assets 'solely in the interests'[194] of the beneficiary and must do so in accordance with an objective standard.[195]

Balkin[196] explores traditional fiduciary-beneficiary relationships, drawing comparisons to the relationship of the technological provider and consumer. He analyses paradigmatic trustees, noting that if confidential information was disclosed in pursuance of a commercial advantage, they would likely be liable for breach of duty.[197] Justifications for the model seek to remedy the relationship asymmetries which are fraught in the data economy,[198] therefore prohibiting exploitation of the vulnerable party. In handling data with consumer welfare in mind, intermediaries are prevented from manipulating data profiles for baser motives.

Privacy-as-Trust decreases the onus currently residing with the consumer. In placing privacy-related decisions with those holding greater knowledge of the decision's outcomes, the traditional provider-consumer relationship is subject to an overhaul. Waldman notes '[u]sing trust as a benchmark for privacy would reorient privacy law away from the narrow focus on individual choice to a broader focus on the relationships that give rise to the disclosure'[199]–it places the impetus on the information intermediaries, relieving the duty of the immobilised individual consumer.

c) Data, as a 'Fictitious Commodity', Should be Afforded Statutory Protection

The dehumanising, corruptive practice of unregulated data extraction has been acknowledged throughout this paper. This paper conjectures that due to the destructive outcomes of the harvesting process, the consumer assumes risk, thus diverging from the myopic view of shareholders as the sole claimants to a firm.[200] This risk justifies the imposition of statutory protection.

To support this claim, the economics of Karl Polanyi shall be invoked. As a critic of Hayek and his ilk, Polanyi denounces *The Road to Serfdom*,[201] focusing on Hayek's inability to account for the self-interest of dominant players,[202] a practice which inevitably engenders crisis and exploits consumers for commercial ends. He retorts that through increased reliance on the utopianism of the market-based system, economic prosperity is not eventuated, but

[194] Uniform Trust Code, Section 802.
[195] ibid Section 804.
[196] Jack M. Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49 UCD L Rev 1183, 1205.
[197] ibid.
[198] Waldman (n 193) 85.
[199] ibid 77.
[200] ibid.
[201] Hayek (n 16).
[202] Karl Polanyi, *The Great Transformation: The Political and Economic Origins of Our Time* (2nd edn, Beacon 2001) 257.

destruction and hardship, much of which is borne by the subordinate person–'[t]o allow the market mechanism to be the sole director of the fate of human beings and their natural environment … would result in the demolition of society'.[203] To expound on his postulation, Polanyi focuses on the idea of the 'fictitious commodity',[204] a material or action not originally produced to be sold in the unregulated marketplace, subsequently undergoing commodification to generate economic value. He labels land, labour, and money as such, noting that prior to refinement, they are simply a measure of human existence.[205] Fundamentally, he accepts the resulting debilitation of the contributing person as axiomatic–consumers become the means to the dominant player's ends in a market-based economy.

Haggart has noted the potential for data to be viewed as a 'fictitious commodity',[206] remarking its quality as a partial form of knowledge; it is a raw material which must be aggregated and refined before its full commercial potential can be realised. Consumers relinquish seemingly innocuous pieces of information online, unaware that human and mechanic aggregation has the potential to, in Polanyian parlance, demolish society. Accounting for the proclivity of conscious and unconscious bias to be reflected in manipulated data, adverse and potentially discriminatory inferences can be made. As an example, Google's image recognition algorithm labelled gorillas as 'black people', a conclusion which likely would not have been reached absent a subjective human input.[207] Furthermore, Facebook's collusion with local police departments relating to the Black Lives Matter movement[208] has sparked claims of 'algoracism'.[209] Both consumer and citizen welfare are jeopardised as prejudice informs the ideals of society and state bodies.

Polanyi also responds to the neoliberal assertion of the curtailing of negative liberty authorised by statist regulation. He refutes the alleged freedom granted by free markets, as freedom is not granted universally.[210] This paper concurs with his thesis–information intermediaries are indeed free in their unfettered corporate discretion but due to imbalances in market power, the individual is not. Rather, Polanyi asserts that liberty of the positive kind is provided by state intervention.[211] Regulated by binding codes, the corporate entity is no longer

[203] ibid 76.
[204] Haggart (n 176).
[205] Polanyi (n 202) 75.
[206] Haggart (n 176).
[207] ibid.
[208] Foroohar (n 1) 238.
[209] ibid 242.
[210] Polanyi (n 202).
[211] Filip (n 19) 73.

afforded discretion in manipulating the human condition for their own commercial ends.[212] By rectifying issues such as the information asymmetry and sanctioning transmission of an intermediary's data practices, the consumer is granted positive liberty as to how they wish to manage their data.

4. Evaluation

As expected, the two opposing arguments are rooted in distinctly different ideals, each having its merits and pitfalls.

The capitalist ideals of wealth generation seem alluring when operating within a vacuum, as it provides simple justification for the corporate objective. However, when the corporate objective is achieved at the expense of human dignity, as it occurs in practice, economic bifurcation cannot be justified. With unfettered innovation promoting outcomes such as the creation of echo chambers and manipulation of vulnerable citizens, it is naïve to uphold the sole primacy of the shareholder within the corporate matrix.

Similarly, invoking the 'difficulty' argument in eschewing state legislation is nothing more than *ignoratio elenchi*. Bipartisanship and ideological divergence do indeed create a hostile environment for universalistic legislation, but this is the case for many types of enacted legislation.[213] Raising these issues does not respond to the question of state-intervention necessity. Resort to law is an extreme measure however, this paper justifies said extremity in protecting ideals core to the Western tradition: equality, democracy, and autonomy.

Furthermore, the argument of liberty as a corollary of market liberalism is fallacious. Bauman correctly notes that the fundamental requirement of a free market is integrity,[214] or rather the 'commitment to promises/contract'.[215] In the absence of this commitment, inequality ensues.[216] This inequality materialises with the ad hoc, sub-optimal application of the FIPs within the privacy policy, precluding the strict knowledge parity necessary for an operative system, thus constituting a market failure. Further market failures arise in relation to property rights, or lack thereof, asserted over data profiles. When the individual cannot adequately assert ownership of his property, he is unable to successfully control its distribution within the market. State intervention is justified on this basis.

---

[212] ibid 78.

[213] For example, gun laws are deeply divisive. However, it has been proven that territories invoking a blanket ban on the aforementioned weapons experienced lower levels of gun violence, suggesting greater citizen protection. See Janet Weiner *et al.*, 'Reducing Firearm Violence: A Research Agenda' (2007) 13(2) Injury Prevention 80, 84.

[214] David Bauman, 'Integrity and Justice: What Is Required of Free Market Participants?' (2017) 3 Palgrave Communications 1, 8.

[215] ibid 6.

[216] ibid 4.

Big Tech's power and ability to 'demolish' society justify the collective being held to statutory account. Viewing data as a 'fictitious commodity' reflects the sentiment that it 'cannot be shoved about, used indiscriminately, or even unused, without also affecting the human individual'.[217] When considered within the wider context, malicious data aggregation has the potential to undermine democracy and equal citizenship. In protection of these higher ideals, state-based regulation is justified.

E. CONCLUSION

This paper explores the insufficiency of the current data protection framework in relation to privacy in the US.

Cultural attitudes towards privacy have undoubtedly informed the system at hand. A main factor in the lack of privacy protection seems to be neoliberalist economic optimism. Additionally, the historic concern of the encroachment of the state into the individual realm, rather than the private corporate entity, has resulted in the development of piecemeal statutes governing public privacy. The resultant attitudes have created distinct legal voids in which individual privacy can be readily violated. Catalysing cultural change is indeed a difficult task, yet Ayres and Braithwaite argue that regulations themselves have a profound effect on institutional structures and corporate cultures.[218] As such, the paper proposes that extraneous state regulation is the most suitable solution.

In analysing the sufficiency of the current market-based framework, the paper explores the open-textured, vague nature of the FIPs. The discussed ambiguity feeds directly into the privacy policy utilised by Big Tech; such terms are thus used to leverage a commercial advantage. The paper concludes that, contrary to what it asserts, Big Tech fails to grant the consumer meaningful 'notice' and 'choice'. The FTC's extraneous inability and internal reluctance to reprimand such actions only serves to exacerbate the problem–corporations are all but discouraged to engage in concealed data practices.

In establishing the insufficiencies of the market-based approach, the paper debates the appropriateness of invoking a state-based approach in protecting privacy. Arguments against regulations prioritise ease, in both judicial and economic terms, as well as the autonomy of the individual and his freedom of choice. However, it is argued that ease is not a sufficient argument when fundamental norms are at stake. The arguments in favour of imposing

[217] Polanyi (n 202) 76.
[218] Ayres and Braithwaite (n 139) 4.

regulation are significantly more compelling in their relation to human dignity, democracy, and integrity.

Although individual autonomy is a primary argument invoked by both pragmatists and fundamentalists, the paper submits that it is an argument more readily bolstered by state-intervention. The opacity of Big Tech's data practices proves Hayek's vision of the autonomous individual as redundant. Rather, the state, in its protectionist capacity, can safeguard consumers, empowering their assertions of positive liberty.

Violating privacy goes to the core of the human condition. It facilitates almost all other aspects of our life, from democratic expression to relationship building. As such, the paper contends that state-based regulation is not merely appropriate, but it is a necessity.