Whose Data? Information Economics, Digital Privacy, and the Right to Be Forgotten

Joel Salazar

ECON 420

December 8, 2021

I. Introduction

The rise of the internet concurrent with and driven by the ascendancy of powerful information technology firms has not been without its issues, controversies, and concerns. "Big Tech" firms such as Facebook, Amazon, Apple, Microsoft, and Netflix have distinguished themselves in the market through satisfying consumer preferences for technology, media, and ultimately information goods (Talocka 2020, Klein 2020). As these firms have gained large market shares, laymen, political pundits, and economists have raised the alarm. Their concern revolves around the idea that these tech firms' activity constitutes a market failure. One common market failure claim leveled at powerful tech firms is a claim of monopoly. Big Tech firms are perceived to command monopoly power harmful to internet users and new entrants in information technology markets (Ghosh and Srinivasan 2020; Petit 2020). A concerned attitude toward Big Tech can be seen in the vernacular that has been coined to refer to Big Tech firms. Jim Cramer, host of CNBC's finance program *Mad Money* created the acronym FAANG in 2017 to refer to Facebook, Amazon, Apple, Netflix, and Google (Fernando, 2021). While creating a shorthand acronym for Big Tech, Cramer also communicated its ability hold a dominating, dangerous share of the market in its jaws. As Big Tech firm's market power has loomed large over users and startups, governments have begun exploring legal and legislative avenues to mitigate the perceived harmful effects of Big Tech's market activities. Much of government foray into Big Tech regulation has also been pushed by competing tech firms looking gain a competitive advantage through rent-seeking activity (Zywicki 2016).

While Big Tech firms receive perennial attention as market failures of monopoly (See Petit (2020), Lamoreoux (2019)), recently more focused attention has been directed toward the data privacy issues of Big Tech. In both popular culture and academic disciplines, the focus has shifted towards these privacy issues. How do firms collect data? Why are firms incentivized to collect data? How does collection of user data violate users' privacy and otherwise negatively impact the individual user and society at large? Are there only negative effects to firm's collection and use of data? In popular culture, heightened awareness of the issues of data privacy are both evidenced and precipitated by media such as the Netflix documentary *The Social Dilemma* released on January 26th, 2020. *The Social Dilemma* explores and dramatizes Big Tech firms' use of data collected from individuals using their platforms to create algorithms that "manipulate users and encourage addiction to their platforms" while "targeting users with ads" (Barnet and Bossio, 2020). In economics and law circles, Caleb S. Fuller notes the "growing topic" of the "economics of digital privacy" (2017). Fuller (2017) and others, notably Alessandro Acquisti et al. (2016), discuss this burgeoning digital privacy literature that has sprung up in the late twentieth and early twenty first centuries.

In this paper I aim to follow the work of Fuller, Klein, Aquisiti and others in exploring the economics of digital privacy to evaluate perceived market failures and policy prescriptions in the digital marketplace. First, I begin with a discussion of Big Tech firms' perceived hand in market failure. Here the paper will provide a literature review of the market failure issues of Big Tech, mentioning the literature evaluating Big Tech firms as monopolies and but primarily offering a survey of the literature focused on

an information economics driven analysis of market failure. After this literature review, my paper will explore proposed intervention solutions to correct the perceived failure of the market to provide data privacy. Included in this exploration are recent appeals in the literature to the necessity of regulatory schemes to "Rein in Big Tech" (Ghosh and Srinivasan, 2021) as well as actual implementation of regulation with a focus on the European General Data Protection Regulation of 2018 and "right to be forgotten laws". After a presentation of the arguments for and examples of government intervention into the digital marketplace, I will explore the works of Fuller (2017, 2018, 2019) and others to show critiques of proposed and implemented privacy interventions and the general "Perils of Privacy Regulation" (Fuller 2017). Here the paper will pivot to discuss the insufficiency of viewing the digital marketplace as a market failure. In this section we will discuss the proper economic framework for evaluation of digital privacy issues, which Fuller (2017) and Acquisti et al (2016) claim is information economics. Following this point my paper will transition to a discussion and evaluation of a particular data privacy intervention, the "right to be forgotten". Klein's (2020) work evaluating fundamental conceptions of information, privacy, and their goods is invaluable in my analysis of the "right to be forgotten". Where I hope this paper contributes to the literature is in an information economics analysis of the "right to be forgotten" laws. I aim to address technological change as part of my work. To this end I offer my thesis: information economics provides the most fruitful framework for analyzing privacy in the digital marketplace (Fuller 2017, Acquisti et al 2016), which suggests that data privacy regulation schemes such as "right to be forgotten" laws are inherently problematic

because they treat essential human problems arising in exchange, accelerated by technology, as novel privacy concerns.

II. Digital Marketplace and Data Privacy as Market Failure

A large portion of the academic literature expressing the zeitgeist of concern surrounding Big Tech market power and violation of digital privacy has categorized these issues as standard issues of market failure. In his 2018 essay, Caleb S. Fuller points to numerous authors holding this view including, Gertz (2002), Newman (2014), (Turow et al 2009), Hoofnagel et al (2012), and Acquisti et al (2016) among others. Arguments of market failure in the digital marketplace aside from the arguments for monopoly taken up by authors such as Nicolas Petit (2020) have primarily focused on asymmetric information between buyers and sellers. The buyers here being the users of online platforms and the sellers being the tech firms that build those online platforms that provide online services. The information asymmetry here lies in users (buyers) being "ignorant of when a firm is collecting information, what information it is collecting, or to what specific uses the information will be put" (Fuller 2019). Hirsch (2010) and Hoofnagle (2005) argue that this information asymmetry causes the digital market to fail as it overproduces data collection and underproduces data privacy "relative to the ideal of perfectly informed market participants" (Fuller 2019). Deleterious effects of this information asymmetry in the digital marketplace are outlined by Acquisti et al (2016) to include "price discrimination in retail markets, quantity discrimination in insurance and credit markets, spam, and risk of identity theft, in addition to the disutility inherent in just not knowing who knows what or how they will use it in the future". The preception

market failure due the nature of asymmetric information in the digital marketplace, specifically in the area of digital privacy, necessitates government intervention to remedy the market failure (Hoofnagle 2004).

An alternative analysis of market failure in the digital marketplace comes from our good friends in behavioral economics. Fuller (2019) points to Calo (2013) who explains market failure in the digital marketplace in terms of tech firms exploiting cognitive biases to find "the specific ways each individual consumer deviates from rational decision making … and leverage that bias to the firm's advantage". Essentially because of the nature of the digital marketplace and its participants, consumers who use Big Tech firm's online platforms are unable to rationally make choices to protect their privacy as these platforms are designed to prey on the cognitive errors and emotional biases of consumers. Alessandro Acquisti (2004) also articulated support for this behavioral economics approach. Behavioral economics and information asymmetry analysis claims help constitute the academic impetus behind data privacy laws such as the European General Data Protection Regulation (GDPR) passed in 2018 and more expansive digital privacy schemes suggested by Ghosh and Srinivasan in their "*The Future of Platform Power: Reining in Big Tech"* (2021).

III. Intervention Attempts at Remedying Market Failure in Digital Privacy

Given the conception of market failure in the market for digital privacy, various policy prescriptions have been suggested and implemented to correct the digital marketplace. Common privacy concerns that regulators aim to address include " the

surreptitious collection of information by internet vendors from visitors to their sites, the sale of that information to third parties, the collection of data from social media accounts, and the use of information gathered online to pinpoint an individual's identity or location" (Fuller 2017). One prominent example of policy intervention in data privacy is the European General Data Protection Regulation (GDPR), drafted by the EU in the mid 2010's and implemented in 2018. The GDPR was born out of the earlier European Data Protection Directive (1995), as an extension of the necessity to protect the "right to privacy" outlined in the 1950 European Convention of Human Rights (Wolford 2019) This regulation placed restriction on what sorts of data firms could collect individuals using their online platforms and required that individuals first give consent before any data could be collected. According the GDPR website, the GDPR "it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU" on penalty of harsh fines up to "tens of millions of euros" (Wolford 2019). By forcing firms to request "unambiguous consent" to collect and process data, the GDPR attempts to rectify the digital marketplace through ensuring that firms do not overproduce data collection while under producing privacy protection. Fuller (2017) comments that "those suggesting regulatory approaches to privacy see regulation as unambiguously welfare-enhancing".

IV. Evaluative Literature of Digital Privacy Regulation

Data Privacy Regulations such as the GDPR have numerous impacts empirically and theoretically. Always present in any government intervention into the economy is the inevitability that the government measure to correct inefficiency will result in further and

likely increased inefficiencies. Government actions are not subject to regulation by profit and loss, and thus government interventions cannot be guided by economic calculation. Government inability to engage in economic calculation prevents intervention solutions from being able to satisfy consumer preferences (Mises 1949, Rothbard 1962, Kirzner 1985, Ikeda 1997, 2005, Fuller 2017). This principle holds in the digital marketplace and the provision of digital privacy. Fuller (2017) explores the implications of government's inherent inability to satisfy consumer preferences by applying the work of Mises (1949), Rothbard (1962), Kirzner (1985), Ikeda (1997, 2005) in market process theory to the digital marketplace. Based his understanding of market process theory rooted in these other authors, Fuller suggests that calls among laymen and academics for "top-down regulatory solutions should be tempered by a full accounting of the costs which this regulation may impose" (2017). To this point Fuller argues that "digital privacy law imposes costs by stifling the unfettered Market Process, by failing to provide an analogue to the market's disciplinary corrective of profit-loss accounting, and by creating superfluous avenues of discovery" (2017). While Fuller (2017) and Acquisti et al (2016) may differ in their conclusions regarding the economics of digital privacy, they both evaluate the idea regulating privacy in terms of tradeoffs and opportunity costs. An example opportunity cost analysis in Acquisti's work comes from an article he co-authored which discusses the tradeoff in implementing data privacy laws governing health information exchanges (HIE). Health information exchanges are "health care information technology" with the "purpose to improve efficiency and quality of care through enhanced sharing of patient data" (Adjerid et al, 2016). Here the authors suggest

that introducing data privacy regulation may encourage some individuals offer up their data in HIEs because the regulation provides assurance of data private data protection. However, Adjerid et al. (2016) recognize that data privacy regulation affects the "availability of [patient] information when it is needed by healthcare providers to make decisions, making promised benefits less likely". Furthermore, "regulation may also increase the cost of establishing and maintaining an HIE (for instance, by imposing additional technological controls or administrative procedures to protect individuals' data)"(Adjerid et al, 2016). Fuller sees the costs of implementing a data privacy law in "the potential to restrict valuable information flows, exacerbate privacy and security risks, raise barriers to entry, increase entrepreneurial uncertainty, and introduce new opportunities for political entrepreneurship" (2017).

Another analysis of data privacy regulation offered by Fuller (2018) is that of "Privacy Law as Price Control". Here Fuller examines the externalities of data privacy laws by evaluating them as price controls. Fuller (2017) like other authors in the literature see the market between internet users (consumers) and internet firms (producers) as one where the internet firms charge a "non-pecuniary 'price'" to use their platforms in exchange for consumer's data to sell to advertisers. Unlike other authors, Fuller argues that by implementing regulation that constrains or prevents user data collection regulators are effectively implementing a price control, as firms are prevented from receiving consumer information in exchange for their services. As Fuller (2017) puts it, digital privacy regulation, "by permitting consumers to side-step this price, effectively offering nothing to the firm in exchange for its services, acts as a price control". As an effective

price control, digital privacy regulation opens the door for the standard price control repercussions such as “tie-in sales, altered investment patters, and adjustments on other margins of exchange” (Fuller 2017). Fuller provides evidence for this claim in the more creative advertising schemes observed in Europe compared to the US by Fulgoni, Morn, and Shaw (2010) as well as tie-in of in-app purchases noticed by Wauters (2014). A further interesting note Fuller makes is that of Buchanan (2008), which suggests the importance of recognizing that firms in operating in the European online markets face “differing constraints” those operating in US online markets. Buchanan (2008) explains this idea as “same players” in with one in a “different game”. Fuller (2017) formulates two implications in his exploration of digital privacy law as a price control. The first is that theory such as price control that “posses a broad consensus” should be brought to bear on issues with less consensus such as the economics of digital privacy. The second implication is that “those arguing for digital privacy regulation should be less confident that digital privacy regulation is welfare-enhancing “ (Fuller, 2017). Fuller notes that it cannot be said that none would be better off as a result of sweeping digital privacy laws, such as those least willing to have data collected on their online activity. Yet, it is impossible to determine if the increase in welfare of the most privacy conscious consumers outweighed the loss in welfare of a “general interest site being force to close” due to lack of revenue a that site’s customers (Fuller 2017). For such an analysis to proceed, interpersonal utility comparisons would be required, which is impossible (Fuller, 2017). Thus, any who considering any foray into data privacy regulation should acknowledge the thoroughly trod economic soil of price-control repercussion as well as

the inherent uncertainty in knowing whether data privacy regulation is truly socially welfare increasing (Fuller 2017).

V. Introduction to the "Right to be Forgotten" Laws

Areas in the economics of data privacy less explored include a analysis of the "right to be forgotten" laws. I aim to contribute to the economic digital privacy literature by addressing this feature of digital privacy policy. "Right to be forgotten" laws are laws that force internet firms such as search engines to remove data about a given individual online at that individual's discretion. These laws have been passed to protect, an individual's control over "their data" as a part of their greater "right to privacy" in the online context. This right has been characterized and defended in news outlets as "the right to have an imperfect past" (Moore, 2017). Proponents of these laws argue that if users of online platforms have information about themselves that they do not want available for access on the internet, whether that information was put online by themselves, or others, they should have the legal right to have that data removed or deleted. At the least, concerned individuals should be able to legally compel search engines to remove links to "their data". Proponents of "right to be forgotten" laws are concerned that access to potentially disparaging personal information without consent violates individuals' privacy and may cause individuals other harms because of a damaged reputation (Moore, 2017).

The "right to be forgotten" has a precedent of being upheld in the court of law in the EU and is codified in EU digital privacy laws as part of the General Data Protection

Regulation (GDPR). *Google Spain SL v. Agencia Española de Protección de Datos,* the case giving the right to be forgotten precedent in the EU, was handed down in 2014. A Spanish lawyer, Mario Costeja was unable to pay a debt in 1998 and had his house repossessed. This sequence of events was recorded in a "local newspaper *La Vanguardia"* (Cunningham, 2017). When Costeja's name was searched in Google, frequently the report of his failure to pay his past debts was at the top of the search results (Cunningham, 2017). Costeja took issue with this and successfully sued Google Spain SL via the Court of Justice of the European Union (CJEU). According to Cunningham (2017), "CJEU ruled that the debt notice could remain on *La Vanguardia's* website, but that Google must delete any link connecting Costeja to it". The codification of this decisions came in 2018 found in Article 17(2) of the GDPR (2018). In the U.S. the "right to be forgotten" has not held up in court though there is survey evidence that a significant portion of the U.S. population thinks the government should support the "right to be forgotten".

VI. Evaluation of the "Right to be Forgotten" Laws

One argument that may be advanced in support of the right to be forgotten laws is that geographic mobility offered "the right to be forgotten" in the past. For example, if someone had a poor reputation in one town due to information possessed by people in that community, the person with the poor reputation could skip town and start fresh elsewhere. In this new town sufficiently distant and disconnected from information exchange with their former town, that individual can build a new identity and reputation for themselves. Depending on the institutional environment, it may be easier or harder for

an individual to assume a new identity. A new identity may be easier or harder to assume based on how many personal papers or documentation are required to operate as a member of a given society. The argument follows that the online environment does not offer this escape as means to secure the "right to be forgotten". A notion exists in public consciousness (Naughton, 2011, Moore, 2017) that once something is online, it never goes away. Given enough search engine queries, anyone with half decent internet connection and a personal computer or phone can dig up all kinds of information on individuals of interest. Data available may often include information that individuals desire to keep out of the public eye and even erase from the public's memory.

Proponents of right to be forgotten laws point to the deleterious effects sensitive information can have on individuals psychological and economic wellbeing. The 2014 court case which brought the discussion of the right to be forgotten to the fore in the EU was the case of an individual, Mario Costeja, who was concerned that information about his severely blemished credit history was readily available to the public. The ready access of this information certainly made his case for future credit approval a weaker one, thus potentially hampering his access to economic goods and overall welfare. The extent to which ready access of his poor credit history caused psychological disutility and social scorn is another potential outcome of the inability to be "forgotten" in the online context. Other areas were an unprotected right to be forgotten would be significant include cases of individuals applying for jobs, seeking admission to universities and other academic institutions, and seeking political office to name a few. All these situations require information about individuals' past actions and characteristics to make decisions that may

affect their welfare. In the age of social media, one overly aggressive, ill-advised, and reactionary tweet can be enough for employers, admissions committees, or constituents to deem an individual unfit for a sought position. In the past, individuals did not have ready access to the amount and scope of information on other individuals that technological change has afforded in our present-day setting. A study by the Society of Human Resource Management (SHRM) found that employers today frequently use "social media for talent acquisition". The survey states that 84% of companies use social media to recruit in their hiring processes and that 43% screen applicants through social media and search engine queries (SHRM, 2018). Online content that poorly reflects individual's aptitude for proficiency in a given job may differ according to the with the industry. However, in applying for any job there is always the potential that employers can find data about an individual that individual did not intend to be part of their job application when they originally posted that data online. Advocates of the right to be forgotten laws argue that it is unjust and a violation of privacy for individuals to be evaluated on the grounds of information that was not specifically surrendered to potential employers for review. Individuals cannot escape the specter of data that is potentially harmful to their psychological, social, and economic wellbeing in the digital context as easily as they were able to in the brick-and-mortar context of the past. Advocates of right to be forgotten laws argue that the specter of an individual's online past is what makes such laws necessary.

This argument that provisions of the "right to be forgotten" through geographic mobility and assumption of new identities is not available in the online context is based

in an insufficient analysis of the online environment and its opportunities to be forgotten. Additionally, the argument does not recognized that fundamental problems of information must be overcome in both the real and digital worlds. The digital world is not unique in presenting us information problems that must be solved for exchange to take place and society to function.

In the online marketplace, individuals can create new identities for themselves, giving themselves an opportunity to be "forgotten". These identities have the same practical implications of moving to a new town, changing one's name, and forming a new identity in a time before the internet. For better or for worse, the digital context makes it easier for individuals to assume new identities and operate as members of the digital society. This idea runs contrary to some scholars' analysis advocating for "right to be forgotten" laws (Dowdell 2016). For example, consider a certain individual who is trying to sell goods on an online platform. Suppose buyers have information that the seller is not to be trusted. If buyers choose not to purchase goods offered by this certain seller based on this bit of information, the individual selling could simply create a new user account under a different username to shake off consumer apprehensions about their trustworthiness as a seller. Without some way of detecting a seller's shift in identity, the same consumers that would not buy from the certain seller originally would likely buy from the seller's new online identity, if their demand for the seller's goods remained the same. In the non-digital setting, it would be much more difficult for a seller to assume a new identity and reap the benefits of a transaction with the same consumer not willing to trade with the original seller's identity based on information possessed about that

identity. Keep in mind also that in both the digital and non-digital contexts the ability individuals have to shift their identities depends on the institutional arrangements discussed by Coase (1997) within those contexts. If a website functioning as a digital marketplace requires that buyers and sellers provide legitimate government identification this will likely make switching between identities more difficult. The economic rules governing exchange and information still hold in the digital marketplace, as does Coase's (1937) principle that it is costly to use the price system. Potential buyers and sellers online have to overcome information asymmetries to facilitate exchange, just as in brick and mortar contexts. Entrepreneurs are capable of this (Fuller 2021), whether it be online platforms creating methods to discourage flight by night sellers or disreputable online vendors creating a new profile to encourage buyers to purchase their goods. No inherent need exists for "right to be forgotten" laws to solve the problems of information asymmetry. Indeed, because right to be forgotten laws are information reducing in nature, it is likely that they will increase potentially harmful information asymmetries, not solve them. The interplay between real and online identities in our world increasingly affects human action and interaction, yet it does not change fundamental problems of information that must be overcome for humans to interact and exchange.

To continue to evaluate the arguments for and evidence presented in support of "right to be forgotten" laws, I think it is essential to further examine the fundamentals of how information is generated and exchanged in the market. A key question in evaluating the idea of a "right to be forgotten" and the greater field of the economics of digital privacy is whether the information that is collected and disseminated in the digital

economy differs from the way information is in the "brick and mortar" economy (Fuller, 2017). Do information economics in the real world hold up in the digital world and in the interactions between the two? Are the economics of digital privacy those of the same economics of brick-and-mortar privacy? Fuller (2017) and Petit (2020) argue that they are.

A key distinction that must be made to provide an economic analysis of privacy issues and policy prescription is the difference between information vs. information goods and privacy vs. privacy goods. As Klein (2020) discusses in his work, we do not purchase information itself but goods that contain them. These information goods include "books, movies, communication infrastructure, consultants, training programs, etc.". Information itself is abstract and immaterial. The only way it means anything and can useful to us is as thoughts in our minds. Mediums of information are information goods which contain stimuli that give rise to certain thoughts in our minds. Information cannot be readily grasped but must be communicated through information goods exchanged in markets. If privacy is the "concealment of information" as Posner (1978) and Stigler (1980) define it, we do not "produce and consume privacy" but "privacy goods: sunglasses, disguises, locks, window shades, land, fences, and in the digital realm, encryption software, cookie blockers, data scramblers, and so on (Klein 2020)". When evaluating issues of information and privacy in economics, it is important to think of information and privacy goods that can be readily subjected to economic analysis, and not in terms of abstract ideas that cannot.

Also germane to an analysis of "right to be forgotten" laws is a discussion of assigning property rights to information and the concealment of information. The notion that individuals can be assigned property rights ownership over information, or the concealment of information is curious. Information is abstract and only means anything and has use value to us in our minds. It is intangible. As Klein states, "information isn't property". In a physical brick-and-mortar setting, if the owner of a store monitors consumer interaction with their products and keeps a record of consumer purchases, this is not a "privacy violation" in the sense that the store infringed on consumer property to take something that was not theirs. Klein (2020) says there is nothing here to steal. The observation of the consumer interacting with products and purchasing some of those products exists in the mind of the store owner and is not a good that the consumer owns. A store owner may keep a written or electronic record of consumers' transactions or record the actions of consumers in their store via video camera. This would constitute the creation of an information good. Yet, the store owner produces this information good containing the "consumer's data" and has property rights over that information good outside of a mutually agreed upon contract stipulating otherwise. The only scenario where the property rights of consumers are violated is the case of contractual breach described by Klein (2020). "Of course, if I have a contract with the grocer that says he will keep my purchase records private, and he shares them with someone else, then I can sue him for breach of contract. But this isn't theft. He hasn't 'stolen' anything; there is nothing for him to steal (Klein 2020)."

This “brick and mortar” analysis extends to the digital sphere. In the digital sphere, websites and other online platforms which record data about their users are analogous to physical stores monitoring actions of their customers. Klein (2020) notes what internet users often consider personal data “is a record of all [their] interactions with platforms, with other users on those platforms, with contractual partners of those platforms, and so on.” Data is “co-created by these interactions” (Klein 2020). Though the context varies, the information generated by user interaction with web platforms and recorded by the web platforms is of the same character as the information that is generated, observed, and recorded by the owners of brick-and-mortar shops. In both cases the “co-created” data of consumer actions in the market is observed and recorded by producers. In both cases the producers record their observations to create information goods in their files whether physical or digital. Users of tech platforms do not possess a reasonable legal property right to these information goods created by tech platforms. The only scenario where consumers do have property rights is if a contract is made between a tech firm and a user of their platform where the firm contractually agrees to not record or disseminate the data generated by the user interaction with its platform, and the tech firm violates this agreement. This example provides an actual violation of rights, the property rights associated with a contract. Klein sums up his fundamental information economics analysis of digital privacy:

> Likewise, “privacy” refers to what other people know about me – it is knowledge in their heads, not mine. Information isn’t property. If I know something about you, that knowledge is in my head; it’s not something I took from you. Of course, if I obtained or used that info in violation of a prior agreement, then I’m guilty of breach, and I use that information to threaten or harass you, I may be guilty of other

> crimes. But the popular idea that tech companies are stealing and profiting from something that's "ours" isn't right.

Using this framework of information, observations, information goods, privacy good, and their relation to property rights articulated by Klein (2020), I would like to give a brief but hopefully helpful analysis as to why proponents of "right to be forgotten laws" and general data privacy regulations consider the digital marketplace to be such a novel environment requiring intervention to correct market failures. If the economics of digital privacy are simply an extension of the economic privacy (Posner (1978, 1981) and Stigler (1980)) in the physical world as Klein (2020) and Fuller (2017) argue, then there is little economically valid impetus for government data privacy regulation, including "right to be forgotten" laws.

Yet some seem to find this economic policy conclusion unsatisfactory. Dowdell (2017) and Ghosh and Srinivasan (2020) advocate for the implementation and expansion of general data privacy regulation, including "right to be forgotten" laws, in the United States and elsewhere. Furthermore, according to a Pew Research Study report from January 2020, 74% of Americans support the "right to be forgotten" (Pew, 2020). A disparity seems to exist between economic analysis of digital privacy and the popular push for heightened data privacy regulation and a "right to be forgotten". Laymen and some academics such as Hoofnagle (2004) seem to view the difference between digital and physical marketplaces to be fundamental. However, a closer look and application of economic analysis suggests that this is not the case. There is no strict dichotomy. Both the physical and digital contexts involve interactions and exchanges between human

beings. The digital context primarily involves remote interactions and exchanges where individuals are not in the same physical location. Yet, in the digital context the interaction and exchanges taking place are still human action and are thus governed by the universal economic principles as outlined by Mises (1946). Remote interactions and exchanges are not something unique to the online environment, as humans have been facilitating interaction and exchange over distances via messengers, letter, smoke signals, etc. for centuries (Kaufer and Karley, 2012). I find that the only difference between the brick-and-mortar contexts and digital contexts is the speed, scope, and amount of information able to be exchanged. Technological change has afforded this increase in speed, scope, and amount of information able to be exchanged. Information that may have taken years to travel between two parties via messenger or letter now takes milliseconds. Information about individual's location and actions can be collected and updated in real time without in-person surveillance. Information that could fill millions of books can now be stored in a thumbnail-sized flash drive and disseminated with the flourish of a keystroke. These vast advances in information technology certainly may heighten the information problems laid out in the economics literature inherent in any human exchange. The extent to which advances in information technology have heightened information economics problems is an open empirical and theoretical question. Yet, the common denominator between in physical brick and mortar contexts and digital contexts is that humans face information problems in their interactions and exchanges. The same basic principles of economics and specifically information economics and its subfield of privacy apply. I do not deny that the changes in information technology do have significant impacts in the

market and on society. However, the extent to which they create novel harms and problems, is only in the sense that they potentially intensify human problems of interaction and exchange that existed prior to the creation of the internet. When weighing the potential increase in problems and harms one must also keep in mind the immense advantage present day information technology offers in facilitating market exchange that increases human welfare. The digital context may also aid entrepreneurs to rise and solve intensified information problems in markets (Fuller, 2021, Klein 2020).

In conclusion, the problems and perceived privacy market failures present in the digital marketplace are extensions of the problems of information economics (Fuller 2017, 2018, 2019; Acquisit et al (2016). As an intervention aimed at privacy, the "right to be forgotten" laws are subject to the tradeoffs and inefficiencies inherent in privacy regulations discussed in Posner (1979), Stigler (1980), Acquisti et al (2016), and Fuller (2017, 2018, 2019). Klein (2020) offers the perspective that there is a lack of theoretical basis for the assignment of property rights over third party observations to the observed individual. Thus the "right to be forgotten" laws are baseless from an economic perspective unless the information individuals wish to be erased from the internet has been disseminated through breach of contract.

VII. Conclusion

The rise of questions surrounding the impacts of technology on markets shows no sign of stopping. Technology, specifically information technology, continues to advance at breakneck pace. These advances will continue to have economic implications and raise

economic questions. Yet as long as human action is involved, essential problems of information must be solved in order to facilitate exchange (Stigler, 1980), no matter the context. Entrepreneurial ingenuity can rise to solve these problems in their various forms and contexts. Regulators attempting to solve these information issues in the digital context must be wary of intervention's inherent inefficiencies in these areas (Fuller 2017, 2018, 2019, Klein 2020), and intervention's potential to distort entrepreneurs' ability solve issues of information and satisfy consumer preferences.

References

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The economics of privacy." *Journal of economic Literature* 54, no. 2 (2016): 442-92.

____. "Privacy in electronic commerce and the economics of immediate gratification." In *Proceedings of the 5th ACM conference on Electronic commerce*, pp. 21-29. 2004.

Adjerid, Idris, Alessandro Acquisti, Rahul Telang, Rema Padman, and Julia Adler-Milstein. "The impact of privacy regulation and technology incentives: The case of health information exchanges." *Management Science* 62, no. 4 (2016): 1042-1063.

Auxier, Brooke. “Most Americans Support Right to Have Some Personal Info Removed from Online Searches.” Pew Research Center. Pew Research Center, August 17, 2020. https://www.pewresearch.org/fact-tank/2020/01/27/most-americans-support-right-to-have-some-personal-info-removed-from-online-searches/.

Barnet, Belinda, and Diana Bossio . “Netflix's the Social Dilemma Highlights the Problem with Social Media, but What's the Solution?” The Conversation. Swinburne University of Technology , February 22, 2021. https://theconversation.com/netflixs-the-social-dilemma-highlights-the-problem-with-social-media-but-whats-the-solution-147351.

Buchanan, James M. “Same Players, Different Game: How Better Rules Make Better Politics.” Constitutional Political Economy 19, no. 3 (2008): 171-179.Coase, Ronald Harry. "The nature of the firm." *economica* 4, no. 16 (1937): 386-405.

Coase, Ronald Harry. "The nature of the firm." *economica* 4, no. 16 (1937): 386-405.

____. “The New Institutional Economics.” *The American Economic Review* 88, no. 2 (1998): 72–74. http://www.jstor.org/stable/116895.

Cunningham, McKay. "Privacy law that does not protect privacy, forgetting the right to be forgotten." *Buff. L. Rev.* 65 (2017): 495.

Dowdell, John W. "An American Right to Be Forgotten." *Tulsa L. Rev.* 52 (2016): 311.

Fernando, Jason. “What Are Faang Stocks?” Investopedia. Investopedia, December 7, 2021. https://www.investopedia.com/terms/f/faang-stocks.asp.

Fulgoni, Gian, Marie Morn, and Mike Shaw. “How Online Advertising Works: Whither the Click in Europe.” comScore. February 2010. http://iabireland.ie/wpcontent/uploads/2012/08/Whither_the_Click_in_Europe.pdf

Fuller, Caleb S. "Is the market for digital privacy a failure?." *Public Choice* 180, no. 3 (2019): 353-381.

____. "Privacy law as price control." *European Journal of Law and Economics* 45, no. 2 (2018): 225-250.

____. "The perils of privacy regulation." *The Review of Austrian Economics* 30, no. 2 (2017): 193-214.

____. “Duckduckgo Can't Exist.” CSOC, July 31, 2021. https://www.centersoc.org/2021/07/31/duckduckgo-and-hostages/.

Gertz, Janet Dean. "The Purloined Personality: Consumer Profiling in Financial Services." San Diego L. Rev. 39 (2002): 943.

Ghosh, Dipayan, and Ramesh Srinivasan. "The Future of Platform Power: Reining In Big Tech." *Journal of Democracy* 32, no. 3 (2021): 163-167.

Hoofnagle, Chris Jay, Ashkan Soltani, Nathaniel Good, Dietrich J. Wambach, and Mika D. Ayenson. “Behavioral Advertising: The Offer You Cannot Refuse.” Harvard Law & Policy Review 6, no. 2 (2012): 273.

____. “Privacy Self Regulation: A Decade of Disappointment.” Consumer Protection in the Age of the ’Information Economy’ (Jane K. Winn, ed.) (Ashgate 2006) (2005).

Ikeda, Sanford. The Dynamics of Interventionism. Advances in Austrian Economics. 2005; 8:21-57)

Kaufer, David S., and Kathleen M. Carley. *Communication at a distance: The influence of print on sociocultural organization and change*. Routledge, 2012.

Kirzner, Israel M. Discovery and the Capitalist Process. University of Chicago Press, 1985.

Klein, Peter. “It's Not So Simple Who Owns ‘Your’ Data.” Truth on the Market, October 22, 2020. https://truthonthemarket.com/author/peterkleinicle/.

Moore, Suzanne. “The Right to Be Forgotten Is the Right to Have an Imperfect Past .” The Guardian. Guardian News and Media, August 7, 2017. https://www.theguardian.com/commentisfree/2017/aug/07/right-to-be-forgotten-data-protection-bill-ownership-identity-facebook-google.

Naughton, John. “Personal Privacy Is a Thing of the Past, so You'd Better Get Used to It .” The Guardian. Guardian News and Media, April 23, 2011. https://www.theguardian.com/commentisfree/2011/apr/24/john-naughton-personal-privacy-mobile-phones.

Newman, Daniel A. "Missing data: Five practical guidelines." *Organizational Research Methods* 17, no. 4 (2014): 372-411.

Petit, Nicolas. *Big Tech and the Digital Economy: The Moligopoly Scenario*. Oxford, United Kingdom: Oxford University Press, 2020.

Posner, Richard A. “Economic Theory of Privacy.” Regulation 2 (1978): 19

Rothbard, Murray Newton. Man, Economy, and State. Vol. 2. Princeton: Van Nostrand, 1962

SHRM. “Using Social Media for Talent Acquisition.” SHRM. SHRM, January 4, 2018. https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/Pages/Social-Media-Recruiting-Screening-2015.aspx.

Stigler, George J. “An Introduction to Privacy in Economics and Politics.” The Journal of Legal Studies (1980): 623-644.

____. “The Economics of Information.” Journal of political economy 69, no. 3 (1961): 213-225.

Talocka, James. “Big Tech and the Sovereign Consumer.” mises.org. Mises Institute, December 14, 2020. https://mises.org/power-market/big-tech-and-sovereign-consumer.

Turow, Joseph, Jennifer King, Chris Jay Hoofnatle, Amy Bleakley, and Michael Hennessy. “Americans Reject Tailored Advertising and Three Activities that Enable It.” Departmental Papers (ASC) (2009): 137.

Von Mises, Ludwig. "Human action." (1949).

Wauters, Robin. “Analysis: An Appraisal of the Burgeoning European ‘App Economy,’ and its Growing Pains.” Tech.eu. Last modified February 13, 2014. http://tech.eu/features/540/analysis-app-economy-europe/Wolford, Ben. “What Is GDPR, the EU's New Data Protection Law?” GDPR.eu, February 13, 2019. https://gdpr.eu/what-is-gdpr/.

Zywicki, Todd. "Rent-seeking, crony capitalism, and the crony constitution." *Supreme Court Economic Review* 23, no. 1 (2016): 77-103.