SPRING 2021

Surveillance Capitalism: Reconceptualizing User Privacy in a New Era of Data Commodification

Perry World House is a center for scholarly inquiry, teaching, research, international exchange, policy engagement, and public outreach on pressing global issues.

Perry World House's mission is to bring the academic knowledge of the University of Pennsylvania to bear on some of the world's most pressing global policy challenges, and to foster international policy engagement within and beyond the Penn community.

Located in the heart of campus at 38th Street and Locust Walk, it draws on the expertise of Penn's 12 schools and numerous globally-oriented research centers to educate the Penn community and prepare students to be well-informed, contributing global citizens. At the same time, Perry World House connects Penn with leading policy experts from around the world to develop and advance innovative policy proposals.

Through its rich programming, Perry World House facilitates critical conversations about global policy challenges and fosters interdisciplinary research on these topics. It presents workshops and colloquia, welcomes distinguished visitors, and produces content for global audiences and policy leaders, so that the knowledge developed at Penn can make an immediate impact around the world.

Perry World House—its programs and the building itself—builds on Penn's strengths in teaching, interdisciplinary scholarship, and policy-relevant research. By doing so, it cultivates the broad worldview, critical thinking, and leadership required to address the most urgent issues of global affairs.

@perryworldhouse

facebook.com/perryworldhouse

@perryworldhouse

Contents

About the Authors

Ali Khambati

Ali Khambati, a rising junior from Texas, studies Finance and Decision-Making with a minor in Data Science in the Wharton School. He is interested in the effects of technological development on international political dynamics, specifically its role in determining the dynamics between high-gross domestic product nations.

Sarah Ko

Sarah Ko is a rising junior studying International Relations and Economics and minoring in French. She works on marketing for The Daily Pennsylvanian and the International Relations Undergraduate Student Association. Interested in global health, Ko is also President of the Student Hospice Organization of Penn.

Chonnipha (Jing Jing) Piriyaltersak

Chonnipha (Jing Jing) Piriyalertsak is a rising sophomore in the College of Arts and Sciences, with academic interests in Philosophy Politics & Economics and History. A native of Thailand, she is a contributor to *The Pennsylvania Punch Bowl* (Penn's first satire magazine) and a Benjamin Franklin Scholar.

Chinaza Ruth Okonkwo

Chinaza Ruth Okonkwo majors in History and Philosophy as a rising junior in the College of Arts and Sciences. She is a Benjamin Franklin Scholar and Robeson Cooper Scholar, involved with the Penn History Review, History Honor Society, CAFSA (Coalition Against Fraternity Sexual Assault), and SCUE (Student Committee on Undergraduate Education). Okonkwo is also the founder of The Black Radical Tradition, a digital and physical radical reading collective.

Guilherme Grupenmacher

Guilherme Grupenmacher, a rising junior from Brazil, is majoring in Philosophy, Politics & Economics in the College of Arts and Sciences. He has previously worked at a think-tank in Brazil conducting research about corruption. Grupenmacher's hobbies include outdoor running, learning new languages, and studying Latin American literature.

Surveillance Capitalism: Reconceptualizing User Privacy in a New Era of Data Commodification

Overview of Problem

The advent of prediction algorithms and deep learning techniques, combined with rapid advances in our ability to collect both structured and unstructured data, has rapidly re-traced the topography of the company-consumer relationship. This revolution in big data can be attributed to advancements in three categories: volume (companies like Walmart collect over 2.5 exabytes of data per day), velocity (real-time collection of data improves the agility of decision-making by corporations), and variety (companies collect data from sources like phones, media, search queries etc.). Not only has this allowed accurate mapping and predicting of consumer journeys, consumer profiles, consumption patterns, but it has also led to the establishment of digital monopolies. Corporations like Google and Facebook offer free services entrapping millions of users while collecting behavioral data on the actions, likes and dislikes of each individual. They then utilize this data to target users with advertisements driving record high revenues. This novel corporate landscape allows the asymmetric retention of power and knowledge to be institutionalized. This not only has dangerous economic implications, but also threatens the implicit right to privacy.

In May 2019, the Canadian government launched a new digital charter where it distinguishes data as a fundamental economic driver of the 21st century.[1] Birch further notes that underpinning the assumption about personal data exploitation in the 21st century is the idea that innovation requires the commercialization of technology. He coined this phenomenon the "innovation-finance nexus". At the heart of this nexus lies practices configured by "rentiership"[2] or the extraction of value through ownership/control of assets. This form of rentiership can be seen by the securitization of IP through the TRIPS regime, where IP has become a tradable asset. He argues that this reclassification drives focus on financial claims to IP rather than the IP itself, necessarily harming innovation. A key distinction between an asset and a commodity is that an asset derives value from its purported future economic revenues. Therefore, politically this requires protection against risks to asset valuation. An example of this trend is Uber, the ride-hailing giant that has yet to turn a profit. Despite recording billions in losses, investors commit capital with the hope of capturing future economic rent once Uber has monopoly power. Uber, and other big-tech monopolies, innovate and grow through different means of rentiership rather than creating value to society.

Not only does the assetization of data hamper beneficial innovation, but it also is conducive to more and more monopolistic practices. Through an analysis of acquisitions by big-tech companies, we can understand the importance of personal data collection within their overarching business models. Over the last 10 years, Facebook has spent billions on the acquisitions of WhatsApp and Instagram to solidify market control and prevent disruption by entrants. Google's acquisition of DeepMind (a British startup) illuminates this desire for rentiership where acquisitions are made solely on the basis of data rights. Political attempts to regulate data are also inhibited by its capitalization because of investment protections designed to reduce expropriations of expected returns. The result is a system where barriers to entry are raised by a monopolization of feedback data by a few large companies inhibiting vertical innovation by startups.

Data has altered the decision-making process for many corporate executives. Google recently completed a $3.2 billion acquisition of Nest to commence its entrance into the thermostat vertical. However, the thermostat industry is not a $3.2 billion opportunity, rather the acquisition was driven by the volumes of data the smart Nest thermostats collect. These platform-based technology companies are able to enjoy the economic advantages provided by vast data collection without protecting privacy creating a negative externality that imposes deadweight loss on society. Consumers suffer from compromised agency and loss of personal sovereignty. Current antitrust lawsuits focus too heavily on supracompetitive pricing that monopolies can charge in the absence of competitors, however privacy violations are inextricably linked to the absence of competitive forces as well. If we think of privacy protections as a nominal tax on big

tech monopolists, they can pass almost the entire nominal amount of the tax to the consumers because they have complete pricing power. A business model that provides free services would not be covered under traditional antitrust statutes that seek to protect the economic interests of consumers.[3] What we are faced with as a society is privacy breaches resulting from market failures, which should be remedied by a combination of regulatory objectives seeking to identify and correct the cause of these imperfect market conditions.

Certain platforms go even further than simply collecting user data and selling it to third parties. In 2014, Facebook conducted a hidden experiment designed to manipulate the emotional expressions of users. Facebook controlled the extent to which people were exposed to particular emotional expressions on their news feeds in order to gauge the corresponding effect on their own emotional state.[4] Companies, not just Facebook, addict younger teens and then gather data on their activities to understand user intent.[5] One question that warrants further research is whether the right to privacy implies a corresponding paramount right to data protection.

Given the existence of a behavioral surplus (the excess of personal data collected with the intent to commodify human behavior) and the long-term ramifications of behavioral exploitation, it is necessary to theorize preventative mechanisms against technocratic control. Now that we have a more in-depth understanding of the economic and social forces resulting in surveillance capitalism, we will begin to explore various policy-oriented solutions. As Zuboff notes, behavioral modification is largely a symptom of an overarching capitalistic desire of profit maximization. Therefore, solutions should attempt to combat this desire on an economic level, removing the link between data exploitation and revenue (or at least minimizing it).

Current Limitations in U.S. Policy

Without a clear framework to regulate these companies' access and usage of users' data, the United States leaves surveillance capitalism largely unchecked. But with companies like Google, Amazon and Apple running our everyday lives, there is undoubtedly a need for a better framework. Similarities have been drawn between these tech giants and traditional monopolies in oil and gas, but the U.S.'s respective responses to each reveal large discrepancies in the digital age. Antitrust suits against Microsoft and more recently Google and Facebook demonstrate the weaknesses in current U.S. policy to maintain the power and influence held by these companies.

In 1998, the Justice Department and coalition of 20 state attorneys sued Microsoft for violating antitrust laws, claiming it was "seeking a new monopoly for its own browser, Internet Explorer"[6] by illegally crushing Netscape, a new competitor. The government eventually won an unpopular battle dismissing the potential threat Microsoft posed: "Holding a triple monopoly (operating system, major applications and the browser), Microsoft would have controlled the future of the web."[7] Despite opening markets up again, allowing for more competition and innovation, much was left the same. It is said that antitrust protections are "too fixated on the idea that the only real harm consists of raising of prices for consumers."[8]

This sentiment is proven by performative efforts to shed light on tech companies' lack of competition and massive influence. Congress has held hearings, most recently with big tech companies, to assess accusations that they've invoked monopoly power. In July 2020, CEOs of Facebook, Amazon, Google and Apple answered before Congress, offering "well-rehearsed lines about how their companies do not tilt the playing field in their own favor."[9] Not much came from this hearing, especially in a virtual format, but Google and Facebook now face antitrust suits from the U.S. Justice Department and various states. The DOJ's suit against Google is focused around their monopolistic power and methods of curbing competition by cutting deals to ensure Google is the default search engine on most devices.[10] Facebook also faces an antitrust suit as the Federal Trade Commission comes together with a coalition of more than 40 states including California. They accuse Facebook of "buying up its rivals to illegally squash competition,"[11] with Instagram and WhatsApp being the most significant acquisitions.

These antitrust suits coupled with performative hearings have done little to ensure users' data privacy and protection. The current patchwork of miscellaneous state and federal responses are not sufficient to prevent monopoly power and infringement of users' rights. It is clear a better, more comprehensive policy is required to move forward. If the Microsoft suit has taught us anything, it is that the impending suits against Google and Facebook and overall

pressure on big tech companies must produce more tangible results. While the FTC remains the main overseer of companies' breaches of privacy, they have faced major pushback from companies claiming they are abusing their authority.[12] The future of technology is contingent on better U.S. policy that is direct about the limitations of these companies.

Latin American:

The negative and sometimes destructive effects of surveillance capitalism has manifested itself on a global scale and different countries have developed methods of accountability to reign in the power of these forces. After it was revealed through documents leaked by former NSA analyst Edward Snowden that the United States had spied on the president of Brazil and collected information from servers like Google, the Brazillian Congress developed an Internet Bill of Rights designed to protect the rights of Brazillian Internet users against government spying and overreach and implementing limits on what corporations have access to. According to Anthony Boadle, "The legislation, dubbed Brazil's 'Internet Constitution,' has been hailed by experts, such as the British physicist and World Wide Web inventor Tim Berners-Lee, for balancing the rights and duties of users, governments and corporations while ensuring the Internet continues to be an open and decentralized network ."[13] Included in the bill are a net neutrality provision, protection of freedom of expression and information and limits on the ability of corporations to gather and use the metadata of Internet users in Brazil among other things. The implications behind this chain of events is critical in analyzing the future of a global order influenced by the pressures of surveillance capitalist corporations. Accusations and proof of spying can have a detrimental impact on the cooperation of governments and distrust in companies that have now become essential to the livelihoods of billions across the globe. There are, however, issues with interpretation and implementation: the judiciary is left to interpret this framework on a case by case basis due to the civil law tradition that does not bind future cases to previous decisions.[14] Legislation like the Brazillian Internet Bill of Rights serve as an example for why this current legislation is not enforceable in the context of the United States and would not solve the issues of a lack of regulation against megacorporations.

EU/GDPR:

In 2018, the Cambridge Analytica scandal brought the dangers of data misuse into the public limelight. A whistleblower working at the British political consulting firm exposed how they had acquired the data of up to 87 million Facebook users,[15] without their clear consent. This data included Facebook likes, personal information from the users' accounts, and the results of a detailed political/personality quiz which the firm had designed. This data was then sold to political groups around the world, including Trump's 2016 Presidential campaign. In spite of the egregious nature of the scandal's large scale implications, Facebook was only fined 500,000 GBP (approximately 643,000 USD) by the British government, as this was the maximum amount possible under UK law.[16]

A few months after the Cambridge Analytica scandal, the European Union implemented the General Data Protection Regulation (GDPR). The GDPR is currently the most comprehensive data protection framework in the world, enforcing a single set of rules for all EU member states.

The GDPR holds companies responsible for ensuring that consumer data is secure, requiring them to perform regular "data protection impact assessments." Data collectors are required to keep internal records of how they use consumers' personal data, and immediately notify data regulators in the event of a data breach. Companies must also maintain transparency with their data operations; consumers are entitled to know how long their personal data will be retained for, and to request specific information on whether their personal data is being processed.[17]

The GDPR also made the consequences for breaching data protection more severe, significantly increasing fines for guilty parties to a maximum of 20 million euros, or 4% of the company's worldwide turnover.[18] Had the GDPR been in place back in 2018, the British government (as a member-state of the EU) could have levied a much harsher penalty on Facebook.

However, the GDPR is not without its faults. It is unclear as to what qualifies as a "reasonable" level of protection for consumer data, giving regulators a lot of power to decide this definition for themselves when assessing fines.[19]

We will explore the GDPR as a model that the United States could adopt, emulating the EU requirements for transparency and

accountability. The GDPR offers clear guidelines for the rights that consumers have over their data, and establishes methods of holding companies accountable for violating these rights— we think the US could benefit from having a similar framework.

Better Framework for Data Regulation is Necessary

Given the alarming signals associated with large corporations and the way our data is being handled, it is clear that some regulation is needed. However, an examination of the current regulatory landscape in America shows that not enough is being done to combat this problem, or to safeguard user privacy. As we look for direction from other countries, we can see initiatives that are steps in the right direction. The GDPR in Europe and the Internet Bill of Rights in Brazil should serve as potential guides for the US in crafting their own data protection framework.

Government-Facing Solutions

Digital Service Taxes

A digital service tax (DST) would tax revenue earned by multinational corporations in digital economy sectors where revenue generation is tied to the activity of their user base. In 2011, the US Congress passed the Digital Goods and Services Tax Fairness Act which provided a legal framework for the implementation of DSTs, but did not go far enough to compel states to pass these taxes. The act also covered physical items that were deemed digital in nature only, and failed to extend to items like advertising, search, or other data monetizing activities. An important note is that a DST is not the same as a tax on corporate profits, but rather is more similar to an excise tax. DST's would be applied to the revenue generated by these activities regardless of their associated costs. Taxes levied on goods and services are passed onto the consumer (depending on the relative elasticities of supply and demand), so imposing a DST could result in higher prices to impose the tax burden on consumers. However, this would be problematic for big tech platforms who market themselves as free options and by extension maximizing consumer surplus. If these companies were to raise prices, they would lose a lot of their customer base, and antitrust regulation would become more promising, which will be discussed in a later section. In order to understand the political and economic implications of a DST in America, we will analyze their effect in countries that have implemented them thus far.

In 2019, Spain imposed a DST of 3% on online advertising, online marketplaces, and data transfer services within Spain.[20] The UK also passed a 2% DST, covering similar activities. While the limited timeframe since implementation poses issues for our analysis, we can see some limited effects. The economic incidence of a DST is likely to be borne by purchasers of the taxable service (for example, companies who pay big tech firms for user data). However, this has a dual effect of reducing demand for user data (via higher prices) and indirectly disincentivizing broad collection and sales of user data. In order to achieve both the economic efficiency gains borne from a DST and more effectively safeguard user privacy, the United States could adopt the following measures:

- Set a Digital Service Tax within a 2-7% range with revenue threshold requirements to target tech giants that enjoy monopoly power in foreign countries.[21]
- Framed as a consumption tax which would cover how much data the Company consumers, rather than how much they profit from the data.
- Modify traditional tax nexus rules by requiring revenue recognition where users are located irrespective of whether the company has physical presence there
- Introduce a tax on the collection, processing and commercial exploitation of user data for companies that have more than a threshold number of users.[22]
- This would effectively account for the role of data in value creative activities and incentivize virtuous behavior at a corporate level.

Pro-competition law for the digital economy

Adapting competition law for the digital economy would consist of a twofold approach: strengthening consumer protection regulations, and promoting a fairer use and exchange of Big Data between the public and private sectors.

Consumer protection regulations would alleviate information asymmetry between users and service providers. The Federal Trade Commission's Guide Concerning The Use of the Word 'Free' currently prohibits products from being marketed as "Free"

when they are "made in connection with the introduction of a new product or service."[23] However, this rule has yet to be applied to zero-price Internet products, such as social media platforms. As a result, online companies are able to describe their products as "free," despite consumers having to pay with their personal data. The FTC's guide also advises that all terms and conditions associated with free products must be "set forth clearly and consistently at the outset of the offer." This is not the case for online services— a 2008 study estimated that each American user would have to spend 201 hours a year to read privacy policies in full detail— on average, this time would be worth about $3,534 annually. Hence, there is a clear opportunity cost that accompanies the lengthy and opaque wording of privacy policies. Economists have proposed a transaction cost economics (TCE) approach, through which companies would have to acknowledge how their products cost consumers their personal data, time and energy comprehending privacy policies, and information security. Based on this analysis, online companies would have to provide users with information on the true cost of these services.

In 2011, the FTC was able to charge Google for engaging in deceptive privacy practices during the launch of Google Buzz (a social networking service); Gmail users were automatically enrolled in the new product, despite seemingly having the option to decline.[24] The FTC's proposed settlement required Google to gain users' consent before sharing information with third parties, particularly if any changes were made to privacy policies as a result of adding or changing features. However, Google violated this settlement in the following year; for enabling tracking cookies on Safari users without their knowledge, the FTC charged a penalty of $22.5 million[25] — the largest ever penalty for violation of an FTC commission, but not a very significant amount for a company such as Google. It is cost-effective for tech companies to engage in illegal behavior, as the revenues far outweigh any legal penalties incurred. Hence, there has to be a longer term solution built into the regulatory framework, which addresses how consumers lack information and agency over their personal data.

- Require companies to recognize that the transfer of personal information is a non-free exchange of value.
- Require online companies to notify users that their access to the service is provided in exchange for their personal data, and tell them what their data is being used for.
- Create a national standard for transparency of contractual terms.
- Give consumers a succinct list of standardized options about the extent to which they allow the collection of their personal data.
- These options must be worded in plain language, to make them more explicit and uniform than how privacy policies are currently written.[26]

Perhaps one of the most significant barriers to effective regulation of Big Data is the gap between the public and private sector. There is undoubtedly a disconnect between the two in determining policy strategies to contain Big Data and ensure user privacy. Bridging the gap between the two will be integral in not only transforming competition law but also enforcing it. The foundation for a relationship is certainly there: In the 2020 election cycle, Big Tech spent $124 million on lobbying and campaign contributions. Of these tech giants, Facebook and Amazon have surpassed Big Oil and Big Tobacco as the two biggest corporate lobbying spenders.[27] Fostering more transparency and clearer boundaries between government and private sector actors will ameliorate concerns over Big Data.

Applying private sector efficiencies to improve public sector mechanisms of collecting and reusing data will be the most pertinent aspect of reconciling this disconnect. Because the government has a greater capacity to collect data on a widespread scale from its gathering of official statistics for public provisional use and for advancing law enforcement, it is already a data-intensive sector of the economy. Exploiting this data for "internal security, crime prevention, health, traffic and even macroeconomic policy"[28] will allow the government to majorly save public funds and further the economy while simultaneously creating substantial competition to counterbalance the private sector. McKinsey estimates from 2011 show the European OECD member states reducing operating expenditures by 15% to 20%, fraud and errors by 30% to 40% and increasing tax collection by 10% to 20%. With an overall gain of 150 to 300 billion euros,[29] exploiting public sector data will not only prove integral to offsetting tech giants but also provide benefits to the public sector as a whole. The U.S. should pursue this opportunity for growth and

potentially work with tech companies to integrate advanced data analysis for public use.

Open Data Initiatives

There are some concerns that doing this would create too much competition so it is imperative that open channels of communication and initiatives to open data across sectors are implemented. Governments can determine the appropriate extent to which data is exploited to ensure a healthy balance between the two. Because the marginal costs of reusing Big Data are so small, it would be beneficial to both sectors to pursue open data initiatives. Making public sector data accessible, with exceptions to safeguard national security interests, will strengthen competitive neutrality. This must be done with extreme care, however, ensuring disclosed data is kept at an aggregate level and privacy safeguards are in place to secure sensitive data. Sensitive data can be classified as, but not limited to, personal information on taxes, health or social transfers. The U.S. should look to previous OECD and CMA recommendations on these initiatives to "[create] simple, fast and less restrictive licensing systems; [enhance] data quality; and [decrease] the price charged per user, if possible to match the marginal cost of maintenance and distribution."[30]

Conversely, private data can also be leveraged for advancing goals in the public sector. Data amassed by private companies often prove useful for the greater public. A prime example of this is the empirical model designed by Ginsberg et al (2009) that leveraged Google's search data to detect and monitor influenza epidemics.[31] This shortened the one to two week lag time of reporting and taking preventive measures by tracking user behavior in real time. There are cases in which private companies may be hesitant to share data with the public sector to maintain their competitive advantage. The OECD recommends efforts be made to circumvent this conflict by incentivizing companies with "pecuniary compensations, fiscal deductions, confidential treatment of data or even data-sharing partnerships between the private and public sectors."[32] In application to the U.S., however, the government should take a more proactive approach. The government can bind companies to comply by threatening to raise taxes.

In each case, making data widely available is key in maintaining neutral competition between the public and private sector. Involving the public sector in data exploitation will balance powerful tech giants. If business models are increasingly reliant on the collection of Big Data, the public sector should pursue initiatives to adapt as well.

Takeaways from the Digital Services Act and Cyberspace Solarium Commission

The rise and widespread development of digital services has resulted in mass digital changes that have a daily and significant impact on life for many. The increasingly diverse ways that are now available for humans to shop, communicate, share and access information are constantly changing, and institutions and governments such as the European Union are developing legislation to keep up with these changes. The Digital Services Act, proposed by the European Commission, is a set of comprehensive rules that regulate the responsibilities of digital services that serve the role of intermediaries between consumers and services. The proposal allows for more protection of consumer rights and less exposure to illegal contents for citizens in an effort towards more democratic control and oversight of the industry. According to the Commission, "The proposal for the Digital Services Act sets out clear due diligence obligations for online platforms and other online intermediaries. For example, under the new rules any user will be able to flag illegal content, and will also have a clear means of contesting platforms' content moderation, both to the platform and through out-of-court mechanisms in their country."[33]

The Digital Services Act and the impact that it will have on citizens and companies in the EU align with the recommendations from the Cyberspace Solarium Commission that seek to better establish greater cybersecurity and change the dynamic between the private sector and government. Utilizing both the impact of the Digital Services Act and recommendations from the Cyberspace Solarium Commission, a possible policy and solution that can work within the United States are first defining digital services in a similar manner to that of the European Commission to create as broad of scope as needed. According to the Act, digital services would include online platforms such as social media networks and markets. Based on the nature of regulation, the United States could seek to expand the scope of this term or utilize the same definition. Furthermore, the Act also places heavier obligations on large platforms and requires more transparency in an effort to understand how online risks

develop. "The proposal also includes measures for cooperation with specialist trusted flaggers and with competent authorities, as well as measures to deter rogue traders from reaching consumers. It offers greater transparency requirements for online platforms about decisions on content removal and moderation, and advertising on online platforms."[34] Lastly, based on the recommendations from the Cyberspace Solarium Commission it may be useful for Congress to establish a National Cyber Director that would serve as a chief advisor to the President for emerging technologies and can therefore more easily engage with the rapid changes that occur in the development of digital services.[35] Increased regulation and protection of consumer rights are needed as digital services continue to grow at an unprecedented rate and have an impact on the daily lives of citizens across the world. It is imperative for governments to begin to create new laws and regulations that keep up to date with new innovations in technology and communications.

The United States can learn a significant amount from the European Union which has already started to develop more comprehensive regulations by gaining inspiration in defining digital services, developing more regulation and transparency from platforms and businesses, and appointing a Director more aligned and focused on emerging technologies.

Engaging the Private Sector in Protecting Data Rights

When it comes to outlining the rights, protections and control over personal information and data rights in the modern world, it comes with no surprise that the private sector plays a central role in helping the world progress into a more equitable information economy. Private sector technology companies, as we will reference these organizations, entail all the private and public companies that provide technology services and as a result generate ownership of personal user data from those who choose to use such services. As of 2019, for instance, 68% of all internet users in the United States were on Facebook, representing the largest share of users by platform, followed by Microsoft and its office management softwares (50%) and Google providing cloud services (30%) and virtual assistants (36%).[36] While these companies still fall under government regulation and must comply with orders that many times affect the way customer data is handled, like for instance, with data mobility restrictions,[37] they still hold majority control over much of the data that their clients are constantly producing, offering a powerful platform for capitalization as well as surveillance regulation. As a result of such influence over the data, which is the building block of most issues that arise with surveillance capitalism, there is a lot the private sector can do to increase transparency, starting with the potential for ripple effects on their dependants, bridging the gap between regulators and innovators, and setting boundaries to work with governments on their technology infrastructures in the first place.

The first point of engagement would be surrounding antitrust competition, where a consolidated number of major players in the space have a profound influence on progressively removing dangerous technology from its services, and should at every given opportunity do so unequivocally. A simple example, for instance, would be a company like Google phasing out third-party tracking cookies in its own browser, Chrome.[38] Such actions generate ripple effects considering the wide coverage that these services and platforms represent. When a change is made in the macro-level of the software ecosystem, many smaller-level services and data points are brought together with it, a simple but effective solution to both concentrate existing customer data as well as protect it from being too widely scattered across platforms. If large software and cloud-based companies come together to implement these policies the effect can be ample in protecting data privacy in the most specific instances, and the public sector can drive this sort of in-house policy development from a recommendation standpoint in setting standards of excellence for the companies that take into consideration its analysis. Nonetheless, corporations still act in the interest of their shareholders, and don't necessarily have to work for the public good, but allowing the government to play a more acting role in compelling them through information awareness and legislation, is an effective way to push for reform.

Another major solution leads to the core of the relationship between government and private sector, and it is the fact that the large technology architects that dominate the industry,[39] and have access to the individual data are many times the ones running the government systems that fiscalize them in the first place. From a legislative perspective, embracing this necessity of tech companies providing services to the federal government and leveraging that to allow for more

transparency between both the public and the private sphere is an important balance to focus on as outlined by experts consulted from different influential private technology companies. In this discourse of symbiotic dependency, it is common to encounter criticisms of issues like regulator-constituent conflict of interest, but there still is an unused potential to set a standard of quality of how organizations and individuals that inevitably interact with technology can be more intelligent about their own data and privacy.

Endnotes

1 https://www.tandfonline.com/doi/full/10.1080/01442872.2020.1748264

2 Referring to data rentiership or the pursuit of innovation strategies designed to capture or extract value through ownership and control of data as an asset

3 https://alsb.wildapricot.org/resources/NP%202019%20Stemler%20ID%2009.pdf

4 https://www.bbc.com/news/technology-28051930

5 https://books.google.com/books?hl=en&lr=&id=l5yeDwAAQBAJ&oi=fnd&pg=PT7&dq=Privacy+AND+Big+Tech&ots=axG7SVmB2D&sig=dJMT3ylouN04utC-MFJ92hhrHqs#v=onepage&q=Privacy%20AND%20Big%20Tech&f=false

6 "Opinion | What the Microsoft Antitrust Case Taught Us - The New York Times," accessed December 11, 2020, https://www.nytimes.com/2018/05/18/opinion/microsoft-antitrust-case.html.

7 "Opinion | What the Microsoft Antitrust Case Taught Us - The New York Times."

8 "Opinion | What the Microsoft Antitrust Case Taught Us - The New York Times."

9 "4 Key Takeaways From Washington's Big Tech Hearing On 'Monopoly Power,'" NPR.org, accessed December 11, 2020, https://www.npr.org/2020/07/30/896952403/4-key-takeaways-from-washingtons-big-tech-hearing-on-monopoly-power.

10 Richard Nieva, "Google's Antitrust Battles: Here's What You Need to Know," CNET, accessed December 11, 2020, https://www.cnet.com/news/googles-antitrust-battles-heres-what-you-need-to-know-faq/.

11 "Facebook Accused of Breaking Antitrust Laws - The New York Times," accessed December 11, 2020, https://www.nytimes.com/2020/12/09/technology/facebook-antitrust-monopoly.html.

12 "Reforming the U.S. Approach to Data Protection and Privacy," Council on Foreign Relations, accessed December 11, 2020, https://www.cfr.org/report/reforming-us-approach-data-protection.

13 https://www.reuters.com/article/us-internet-brazil/brazilian-congress-passes-internet-bill-of-rights-idUSBREA3M00Y20140423

14 Carolina Rossini, Francisco Brito Cruz, and Danilo Doneda, "The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet," September 29, 2015, https://www.cigionline.org/publications/strengths-and-weaknesses-brazilian-internet-bill-rights-examining-human-rights.

15 Hanna Kozlowska, "The Cambridge Analytica scandal affected nearly 40 million more people than we thought," QZ, accessed December 11, 2020 https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says/

16 Paolo Zialcita, "Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal," NPR, accessed December 11, 2020 https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal#:~:text=Facebook%20has%20agreed%20to%20pay%20a%20%C2%A3500%2C000%20(about%20%24643%2C000,media%20data%20for%20political%20purposes.

17 Judy Schmitt, "How the Proposed EU Data Protection Regulation Is Creating a Ripple Effect Worldwide," Privacy Association, accessed December 11, 2020, https://iapp.org/media/presentations/A12_EU_DP_Regulation_PPT.pdf

18 "Regulation (EU) 2016/679 of the European Parliament and of the Council," Official Journal of the European Union, accessed December 11, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e6226-1-1

19 "Top five concerns with GDPR compliance," Thomson Reuters, accessed December 11, 2020, https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance

20 Lowry, Sean, "Digital Services Taxes (DSTs): Policy and Economic Analysis", Congressional Research Service, Accessed Wednesday, March 31st, https://fas.org/sgp/crs/misc/R45532.pdf

21 Young, Ran Kim, "Digital Services Tax: A Cross-Border Variation of the Consumption Tax Debate", Utah Law Digital Commons, Accessed Wednesday, March 31st, https://dc.law.utah.edu/cgi/viewcontent.cgi?article=1211&context=scholarship

22 De Filippi, Primavera, "Taxing the cloud: introducing a new taxation system on data collection?", Internet Policy Review, Accessed Wednesday, March 31st, https://policyreview.info/articles/analysis/taxing-cloud-introducing-new-taxation-system-data-collection

23 "Guide Concerning Use of the Word 'Free' and Similar Representations", Electronic Code of Federal Regulations, Accessed Wednesday, March 31st, https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=4c2a16712079bc4bcaa6fed5899c2537&mc=true&n=pt16.1.251&r=PART&ty=HTML

24 "FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network", Federal Trade Commission, Accessed Wednesday, March 31st, https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz

25 "Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser", Federal Trade Commission, Accessed Wednesday, March 31st, https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

26 OECD Secretariat, "Big Data: Bringing Competition to the Digital Era", Organisation for Economic Co-operation and Development, October 27 2016, https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

27 "Big Tech, Big Cash: Washington's New Power Players," Public Citizen, accessed April 1, 2021, https://www.citizen.org/article/big-tech-lobbying-update/.

28 OECD Secretariat, "Big Data: Bringing Competition to the Digital Era", Organisation for Economic Co-operation and Development, October 27 2016, https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

29 OECD Secretariat, "Big Data: Bringing Competition to the Digital Era", Organisation for Economic Co-operation and Development, October 27 2016, https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

30 OECD Secretariat, "Big Data: Bringing Competition to the Digital Era", Organisation for Economic Co-operation and Development, October 27 2016, https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

31 OECD Secretariat, "Big Data: Bringing Competition to the Digital Era", Organisation for Economic Co-operation and Development, October 27 2016, https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

32 OECD Secretariat, "Big Data: Bringing Competition to the Digital Era", Organisation for Economic Co-operation and Development, October 27 2016, https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf

33 https://ec.europa.eu/digital-single-market/en/digital-services-act-package

34 https://ec.europa.eu/digital-single-market/en/faq/faq-digital-services-act

35 https://www.solarium.gov/report

36 Esther Shaulova and Lodovica Biagi, "Tech Giants in the U.S. 2019 Report," Statista, accessed April 1, 2021, https://www.statista.com/study/63116/tech-giants-in-the-us-report/.

37 "The Value and Challenges of Regulating Big Tech," Harvard Kennedy School, accessed April 1, 2021, https://www.hks.harvard.edu/faculty-research/policy-topics/business-regulation/value-and-challenges-regulating-big-tech.

38 Gary Guthrie Reporter and Gary Guthrie Gary Guthrie covers technology and travel for the ConsumerAffairs news team. Prior to ConsumerAffairs, "Google to Phase out Third-Party Tracking Cookies in Its Chrome Browser," ConsumerAffairs, accessed April 1, 2021, https://www.consumeraffairs.com/news/google-to-phase-out-third-party-tracking-cookies-in-its-chrome-browser-012521.html.

39 Alex Engler, "Tech Cannot Be Governed without Access to Its Data," Brookings (Brookings, September 10, 2020), https://www.brookings.edu/blog/techtank/2020/09/10/tech-cannot-be-governed-without-access-to-its-data/.

PERRY
WORLD
HOUSE
University of Pennsylvania

UNIVERSITY OF PENNSYLVANIA
PERRY WORLD HOUSE

3803 LOCUST WALK, PHILADELPHIA,
PA 19104

215.573.5730