Corporations, Consumers, and Control:

Data Privacy and the Role of the Federal Government

We, as Americans, rely on the Internet. We use it to shop, communicate, and pay taxes. We use it to showcase our lives and escape reality, and we do it all without paying heed to the consequences of constantly using such a system that profits off of our dependence on it. Digital footprints are the most vulnerable and revealing elements of the Internet, and unfortunately, they are also the most unprotected.

Everybody has clicked "Accept" on a popup to sites they expected to spend less than five minutes on. However, in that split second, their automatic response to an annoying banner allowed the website's host to track their every move, compile a description of the user's interests, and potentially sell that information to other companies, who combine it with *their* information on the user. The process repeats trillions of times a day for billions of users. Some websites don't ask for permission, yet collect the data anyway. Setting social media posts to "friends only" doesn't stop the company from gathering where you are, how often you go there, who you went with, and what you're doing. The recent Facebook-Cambridge Analytica affair put the looming data privacy controversy front and center by revealing exactly how much a company can gather on its users without their knowledge, and perhaps more importantly, what it can *do* with that information. Cambridge Analytica took data on millions of Facebook users without their consent and used it for political advertisement (Garret). In the wake of the scandal, Pew Research Center found that 81% of Americans felt that they had little or no control over the data that companies collect on them. 79% said they were concerned about how their data was being

used. Americans will never stop using the Internet, but their data needs to be protected, and I believe it is up to the federal government to do so. The primary duty of the government should always be to protect its constituents, and right now, its constituents are, simply put, fearful. The government has actively ignored the corporate data privacy issue for years and put it behind the more "real" threats of bombs and radical extremism. In their War on Terror, the government has consistently, year after year, administration after administration, failed to terminate the greatest threat to the American people: the domestic terrorists we call big business.

There have been previous attempts to at least acknowledge data privacy by various politicians, but every time, they have been overlooked and never actually implemented. The Obama administration issued a Consumer Bill of Rights that listed rules for organizations to follow, essentially saying they must allow consumers to regulate more of their own data, develop a "code of conduct" concerning data, and have greater security on user data (EPIC). However, CPBORA had no way of enforcing any of its suggestions and was criticized for advocating for tech companies to regulate *themselves* without the involvement of the government on any level. Other endeavors at securing data privacy include Senator Maria Cantwell's Consumer Online Privacy Rights Act (COPRA) and Senator Kirsten Gillibrand's Data Protection Act (DPA), both drafted in the last six months and both expected to fail to become law. COPRA would allow states to create their own laws and enforce them on their own, and DPA seeks to establish a Data Protection Agency that would settle civil suits against companies concerning the use of data.

Neither of these bills are enough.

What America needs to give its people is a program that would implement data protection policies at a *federal* level, with laws to check corporations and recognition of privacy as a

citizen's right. The European Union has faced the data privacy issue face-on with its General Data Protection Regulation (GDPR), which gives control of data back to the user (Kersten). The beauty of the GDPR lies in its collaboration between what it calls "data culture" — individuals, data protection officers, corporations, and the European Commission. Fines for violating it rise up to four percent of a company's annual earnings, a substantial amount that businesses cannot afford to lose (European Commission). The threat of such a blow to their earnings intimidates enterprises, and they are forced to comply with the provisions of the GDPR and give control of data back to the user.

The genius of the GDPR has made it the stricted and far-reaching data privacy regulation in the globe, and I believe the United States must emulate it. The great state of California has implemented its Consumer Privacy Act, heavily based on the GDPR, which allows users full transparency on data collected from them by companies (Paul). They can instruct companies not to sell their data or delete their data altogether. With such a method of governance applied nationally, citizens of America would finally feel in control of their online presence. However, that's not the only benefit. A national data privacy system will increase consumer trust, which would increase revenue for companies; an Accenture survey concluded that 58% of consumers would spend more on providers that enhance experiences without compromising privacy. With greater consumer trust, greater business earnings, and greater oversight on data, an enforceable federal data privacy policy is in the best interest of all parties.

It's no secret that our online presence tells more about us than we know ourselves. Every minute we stay on the Internet, information is collected on us on an unimaginable scale, and big business uses it to thrive. However, instead of being complicit in the vicious cycle of data theft

orchestrated by corporations, the federal government must do what it's meant to do and serve the *people.* A comprehensive data privacy system has been neglected for decades. While creating one and enforcing it will take time and patience, tomorrow will be too late. The data of the American people needs to be protected *today* — and the federal government has the complete power to do so.

Works Cited

Auxier, Brooke, et al. “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.” *Pew Research Center: Internet, Science & Tech*, Pew Research Center, 31 Dec. 2019, www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Center, Electronic Privacy Information. “EPIC - White House: Consumer Privacy Bill of Rights.” *Electronic Privacy Information Center*, epic.org/privacy/white_house_consumer_privacy_.html.

Garret, Goeffrey. “Data Privacy After Cambridge Analytica.” *Wharton Magazine*, 3 May 2018, magazine.wharton.upenn.edu/digital/the-politics-of-data-privacy-in-a-post-cambridge-analytica-world/.

“Data Protection in the EU.” *European Commission - European Commission*, 19 Feb. 2020, ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

Kersten, Jenna. “Who's Enforcing GDPR? - European Data Protection Board: KirkpatrickPrice.” *KirkpatrickPrice Home*, Jenna Kersten Https://Secureservercdn.net/198.71.233.41/27f.9c9.Myftpupload.com/Wp-Content/Uploads/2016/06/KirkpatrickPrice_Logo.Png, 3 Mar. 2020, kirkpatrickprice.com/blog/whos-enforcing-gdpr/.

Mullahy, Tim. “A New Era of Privacy – Why Regulations like the GDPR Are Actually a Good Thing for Your Business.” *CPO Magazine*, 28 May 2019, www.cpomagazine.com/data-protection/a-new-era-of-privacy-why-regulations-like-the-gd

pr-are-actually-a-good-thing-for-your-business/.

Palmer, Danny. “What Is GDPR? Everything You Need to Know about the New General Data Protection Regulations.” *ZDNet*, ZDNet, 17 May 2019, www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.

Paul, Kari. “California's Groundbreaking Privacy Law Takes Effect in January. What Does It Do?” *The Guardian*, Guardian News and Media, 30 Dec. 2019, www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do.