C. Kaysen
New York, NY 10013

November 9, 2018

National Telecommunications & Information Administration ("NTIA")
1401 Constitution Ave., N.W., Room 4897
Washington, D.C.

Re: No. 180821780-8780-01

Dear NTIA:

I am writing to call the NTIA to action in researching the implications of a measure President Trump signed in April of 2017.

1. Call For Action

In consideration of the principles laid out in the NTIA's proposed approach to consumer data privacy, I am urging the NTIA to act on a recent law that devastates consumer privacy. On April 3, 2017, President Trump signed a measure reversing rules that would have required internet providers to obtain a user's consent before selling their browsing history to third parties. [1]

The law grants new freedom to Internet Service Providers ("ISP") to collect and sell information such as our Web browsing history and app usage. The law serves as a devastating blow to privacy rights and our country's most precious values. In the pursuit of collecting our data, ISP's are flagrantly violating our privacy and effectively monetizing our lives. Our privacy should be treated as a paramount human right, and ISP's are now given free rein to treat it as a commodity. [2]

In this call for action, I will elucidate the contentious debate surrounding consumer privacy and data collection, the harms of allowing ISP's to sell consumer data, the legal framework that exists and the inadequacies of American law in dealing with consumer privacy. I will examine the leading theories on

[1] Jerry Hildenbrand Does Google sell your personal data? Android Central (Jan. 12, 2018), https://www.androidcentral.com/does-google-sell-your-data (last visited Nov. 8, 2018).
[2] Xfinity What are Internet Service Providers Comcast Corporation (Jul. 6, 2017), https://www.xfinity.com/hub/internet/internet-service-providers (last visited Nov. 8, 2018).

building a new framework. I will put forth my recommendations of the principles that must be implemented in order to fully realize the NTIA's proposed outcomes.[3]

2. Introduction

Our world exists at our fingertips. From our Tinder app which we use to spark social connections, to the WebMD page we rely on to research our medical symptoms, to our phone's GPS which navigates our walk home, technology is embedded in every aspect of our lives. In an instant, our personal information moves across the vast landscape of technology. The information our data can reveal about us can give a profoundly intimate look into our lives. It runs the gamut from our spending habits to our sexual preferences to our medical conditions to our political affiliations. [4]

ISP's who sell our data claim that it is anonymous and aggregated data. Research has shown us that we should be weary of these claims, as even anonymous data can be used to form unique data sets. This information can be used to paint an intricate portrait of who we are. ISP's collect thousands of data points about us, and if the price is right, ISP's can now sell them without our consent.[5][6]

3. Case Study: Eckert and Dews Research

German television journalist Sea Eckert and data scientist Andreas Dews tested the veracity of the claims of ISP's who sell user data for a feature called "Naked on The Net", which aired on the German television news magazine Panorama in November 2016. Eckert and Dews used a method developed in 2008 by data scientists at the University of Texas. To obtain data for their research, Eckert and fellow reporters created a fake online-marketing firm and approached data brokers with an interest to buy browsing data.

---

[3] Google How to use SEO? Google, Inc. (Nov. 8, 2017), https://support.google.com/webmasters/answer/35291?hl=en (last visited Nov. 8, 2018).

[4] Brian Feldman Anonymous' Browsing Data Isn't As Anonymous As You Think, Intelligencer (Aug. 1, 2017), http://nymag.com/intelligencer/2017/08/anonymous-browsing-data-isnt-as-anonymous-as-you-think.html (last visited Nov. 8, 2018).

[5] Bruce Scheier Why anonymous data sometimes isn't, Intelligencer (Dec. 12, 2017), https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/ (last visited Nov. 8, 2018).

[6] Barry Schwartz Google Search Console Reports Removes Anonymous Queries Search Engine Roundtable (Aug. 27, 2018), https://www.seroundtable.com/google-search-console-reports-anonymous-query-26273.html (last visited Nov. 8, 2018).

They used a fake computer program to sift through the data. They were able to generate exact matches of data with individual profiles. They were able to ascertain user's names, locations, and minutiae of their internet activity.

ISP's may argue that the aggregation of consumer data is innocuous, however, as Dews and Eckert demonstrated it places consumers at a significant risk. The collection, storage, and commercialization of consumer data leaves ample opportunity for privacy violations and blackmail, when data is compromised or hacked by morally unscrupulous individuals and groups.

4. Arguments for Commercialization of Data

Proponents of the commercialization of data may argue that consumer privacy is a sliding scale. They may argue there an alignment of incentives at play and that privacy and data embodies a tradeoff and an exchange. Our information becomes commercialized and we get free, more targeted services in return. If our information was not commercialized, we would likely need to pay for the service and it wouldn't be as optimized.[7] Proponents may argue that the same issues generated by commercializing data also create equality. They make it cheaper for smaller businesses and smaller political big money to compete with large business and large political donors. Data is powerful, but it can give little people that understand their audience an effective leg up.

5. Social Costs of Selling Our Data

Privacy advocates have espoused that the commercialization of data perpetuates discriminatory behavior shaping and categorization, which inflicts social costs. They contend that we can discern information about people from their search history, and this has dangerous impacts on society. From analyzing a user's data we can determine their sexuality. We can know their disability status. We can know they donate to Planned Parenthood. We can figure out who's connected to which social networks and

[7] Ashley Carman People are getting locked out of innocuous Google Docs for supposedly violating Terms of Service The Verge (Oct. 31, 2018), https://www.theverge.com/2017/10/31/16581406/google-docs-error-terms-of-service-lock-out?fbclid=IwAR1uWy4sdlyV0Ptj2Dj7tybS8z8vpHmK8hw675Phraq-hXhZaIX6bARCB7s (last visited Nov. 8, 2018).

political groupons. We are able to put labels on people, making it easier to discriminate against them thereby wedging a larger social divide. This information could be used by hate groups, by government agencies, by anyone who seeks to inflict harm. Ad targeting can be at the detriment of religious and ethnic minorities, immigrants, and LGBTQ individuals. This is an especially prescient concern as we debate DOCA and birthright citizenship.[8]

When companies sell our data, they are violating our trust. This disrupts social cohesion and has far reaching impacts on our institutions. As propounded by Douglas North in Institutions, Institutional Change and Economic performance. If people don't trust each other it increases transaction costs. There are More lawyers and security guards and more time setting up procedures and oversight etc.[9]

6. Data Collection- California Law

In the United States, privacy is not viewed as a human right. Rather, data privacy laws are sparse, and those that do exist are deficient when it comes to limiting what companies are capable of doing with our information. In June 2018, California passed a monumental digital privacy law granting consumers more control over and insight into the spread of their personal information online.

California's recently passed Consumer Privacy Act will require certain businesses to give user's the choice to opt in or opt out of selling data. The act will go into effect January 1, 2020. Under the Act, ISPs must them publish privacy policy, discuss specific themes in policy, what info they collect and with whom they share it. ISP's will also need to share the privacy data they collected to consumers. Under the Act, companies must still give consumers who opt out the same quality of service. [10]

---

[8] Emma Woollacott Facebook Forced to end discriminatory ad-targeting across the U.S. Forbes (Jul. 25, 2018), https://www.forbes.com/sites/emmawoollacott/2018/07/25/facebook-forced-to-end-discriminatory-ad-targeting-across-u-s/#6888ecbb4424 (last visited Nov. 8, 2018).

[9] Douglas North Institutions, Institutional Change, and Economic Performance Journal of Economics (Jan. 3, 2018), http://kysq.org/docs/North_91_Institutions.pdf (last visited Nov. 8, 2018).

[10] Daisuke Wakabayashi California Passes Sweeping Law New York Times (Jun. 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html?fbclid=IwAR0YIDi66m_WyaFjhJ0jjQtSo9EbsmyJJuZJJjuSDCcqmce1ufvGIbtiIVM (last visited Nov. 8, 2018).

Already in effect is California's Data breach notification law, which provides that as soon as a company knows of a data breach they must notify victims of that data breach. This aligns with the NTIA's desired outcome of managing risk. California's Consumer Privacy Act and breach notification law are steps forward in the right direction. There is optimism that more states will adopt these principles over time and there will be a nationwide standard. Nevertheless, greater, more expansive efforts must be made in order to build a truly consumer-oriented data privacy framework

In practice, ISP's operating under a truly consumer-oriented data privacy framework would abide by all the required provisions of state law and goes beyond that to explain the use in a way that is specifically tailored to their sites. They would be transparent in its endeavors. Their privacy policies would be accessible, open, and transparent and they would not mislead consumers for personal gain. [11]

7. Contract Law

We live in a world where we have a dominant paradigm of thinking of consumer privacy in terms of contract law. American law dictates that the commercialization of our search histories is permissible under contracts. The dominant view is that we're consenting to the commercialization of our data. I would argue that by not opting in, we are not truly consenting. Moreover, consumers can consent to selling our data now, but these terms may change. Consent is not for perpetuity.[12]

Contract law is proving to be an inadequate rule for thinking of consumer privacy rights. Traditional paradigm is problematic. It is insufficient for the complex, ever evolving world we live in. We need a different way of thinking of this. Contract law is not the right paradigm. We need legislation. The better model for this is fiduciary duty law. When we use the services of a physician we are relying on them. We are entrusting them with our lives. The law therefore recognizes there is a fiduciary obligation that doctors must act in our best interest.

---

[11] Chris lp Ashley Madison Engadget (Mar. 29, 2018), https://www.engadget.com/2018/03/29/ashley-madison-president-comeback-interview/ (last visited Nov. 8, 2018).

[12] Priscilla The Privacy Torts Pricilla.org (Dec. 12, 2017), http://www.privacilla.org/business/privacytorts.html (last visited Nov. 8, 2018).

In this technological age, ISP's are similarly a public utility. We trust ISP's with our most intimate information. ISP's should thus have an elevated status in the eyes of the law. There is currently no requirement ISP's uses our information in our best interest or consults with us for it. As Ari Waldman posits in his book *Privacy as Trust*, treating companies who collect our data as fiduciaries would be a superior framework. [13] The NTIA should adapt a paradigm of companies as our trust fiduciaries. Additionally, The NTIA should orient its efforts towards advancing regulation that cultivates consumer trust.

8. General Data Protection Regulation

In the European Union (EU), privacy is conceived of as a human right and this informs their culture, institutions, legal framework and social mores regarding consumer privacy Their approach is shift from a capitalist concept of our ownership of data and ability to profit of it. This is embodied by the GDPR.

The General Data Protection Regulation ("GDPR") is a set of laws which regulates the means through which technology companies may collect, store and use personal data. The GDPR concerns the processing of personal data and the rules relating to the free movement of personal data. The GDPR covers all individuals within the European Economic Area. The GDPR is pushing privacy in the right direction and as time and technology evolves, there will be more privacy regimes in place in other countries. The NTIA should learn from the GDPR and adapt its principles.

Article 25 of the GDPR provides for the protection of data by design and default. Data by design requires appropriate measures be taken throughout the entire life cycle of the product to avoid violations of privacy. Here, data by design means that ISP's should put in place safeguards against manipulating a user's identity from the beginning to end of the search engines life cycle technology. This means ISP's should have opt in clauses, protect their user data. They should ensure user data is not pseudonymized and unable

[13] Ari Waldman, Privacy as Trust: Information Privacy for an information Age Cambridge University Press (Mar. 29, 2018), https://www.cambridge.org/core/books/privacy-as-trust/C5F22BAD9EB53AF6C4098D8FC5B64C81 (last visited Nov. 8, 2018).

to create unique user profiles. The NTIA should especially take note of the GDPR's emphasis on obtaining express consent of users over implied consent.

Data privacy by default means that only necessary personal data is collected, stored, or processed and personal data is not accessible to an indefinite number of people. Here, ISP's should be able to protect against unnecessary personal data by requiring consent and notice of cookies that collect personal data not necessary to make the website function.[14]

Regulators are evolving towards a global standard with principles, such as Federal Information Processing Standards ("FIPPS"). The NTIA should take note from the GDPR and give special categories to data and give certain categories higher protection. Consumer privacy regime is naturally evolving from a sector specific framework to a global overarching idea and there should be flexibility to innovate.[15] [16]

9. Implementation

ISP's who commercialize user data should orient their efforts, policies, and infrastructure towards reaching the NTIA's desired outcomes. ISPs can achieve the NTIA's desired outcomes by implementing privacy by design as their ethos. Privacy by design means that ISP's should value their user's choice and consent above any shareholder interest. They should foster active engagement with their users, and a relationship fortified by trust, honesty and integrity. Privacy policies are an opportunity for companies to give consumers notice and choice in a way that is transparent. Notice and choice are lacking when ISP's sell our search history. [17]

---

[14] Google How Google uses cookies Google, Inc. (Nov. 8, 2017), https://policies.google.com/technologies/cookies?hl=en (last visited Nov. 8, 2018).
[15] The European Union GDPR European Union (Nov. 8, 2018), https://eugdpr.org/ (last visited Nov. 8, 2018).
[16] Homeland Security Fair Information Practice Principles Homeland Security (Nov. 8, 2017), https://www.dhs.gov/publication/fair-information-practice-principles-fipps (last visited Nov. 8, 2018).
[17] Kim Zetter Hackers Finally Post Stolen Ashley Madison Data The Verge (Aug. 18, 2015), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/?fbclid=IwAR0Dq4jvieBwJ6Ns0ltYVQIWqe34ivINfDtBA9zZGbWbm-5oNjptCcWsx3g (last visited Nov. 8, 2018).

To reach the NTIA's desired outcome of transparency, ISP's should clearly delicate in their privacy policy the specific means through which they are collecting data. They should also articulate exactly what data they're using, and how they intend to use it. Their privacy policy should not consist of vacuous language. A consumer-oriented privacy policy puts thought and tailored content.

ISP's should have opt-in clauses rather than opt out clauses to allow companies to sell user data. Contracts with opt out clauses empowers consumers by giving them choice. Through opt out clauses, there is less asymmetry and power imbalance between the consumer and the company. Users should have control over the personal information they provide. Users need to be able to decide if a company can store and sell their day. Our choice and freedom should not be a commodity we compromise for optimized search results or more convenient browsing options. [18]

Privacy by design also means that ISP's must manage risk. In managing risk, ISP's should have investigators and infrastructure in pace to ensure the data truly is anonymous. Organizations should manage risk and enforce security safeguards. Employees of ISP's should undergo special training.

Holding ISP's accountable comes at the consumer and government level. As consumers we can hold companies accountable by mobilizing and voting on laws that protect our data. The government can hold companies accountable with regulation, law and best industry practices. We should empower ISP's to make ethically informed decisions. We can advance towards a world where our privacy is a human right and not a luxury good.

10. Public Policy Argument

The NTIA should demand more transparency and accountability about the potential impacts on human rights that can result from the collection and commodification of our data. Commercializing our search history may be good for shareholders but may be bad for humanity. Allowing companies to sell our data can lead to the suppression of free speech. ISPs such as Google can use our data to control our

[18] Google AdWords Google, Inc. (Nov. 8, 2017), https://ads.google.com/home/ (last visited Nov. 8, 2018).

conversation. They can threaten our free and independent access to media. The Cambridge Analytica and Fake News scandal embodied this. There was political manipulation of Facebook because of Facebook's algorithm. This in turn affected politics and news exposure. Facebook's' power to collect and sell our data wielded immense social and political impacts. [19]

ISP's can also use our data to censor us. Google has used artificial intelligence in the past to comb private data and ban people from their private emails and private Google Drives because of content that they politically disagreed with. By allowing ISPs to monetize our search history, every company can effectively act as a government once they get a certain percentage of market share.

The commercialization of data inflicts harm when ISP's sells to governments and companies that aim to suppress human rights and undermine freedom of expression. This harm was realized when Google used their data to create a censored search engine for China. [20] Google also sold data to a Chinese search engine, Dragonfly, who used it to monitor users. Their search engine hides search results that China's authoritarian government wants to suppress, including "information about democracy, free speech, peaceful protest, and human rights, according to an investigation by *The Intercept."*[21] In response, organizations such as Amnesty International and Human Rights Watch penned a letter urging Google CEO Sundar Pichai to terminate the project. They wrote, "Google risks becoming complicit in the Chinese government's repression of freedom of speech and human rights in China."[21] The internet should be a liberating forum, but when we allow companies to collect and sell our data, we jeopardize our human rights.

3. Conclusion

Privacy is not a Utopian narrative. The NTIA has the power to galvanize real change and set higher standards for consumer privacy. In the spirit of innovation and advancing towards a bright future for privacy, The NTIA should act on the recent legislation that emboldens ISP's to sell our search history. The

[19] Google Search Engine Optimization Starter Guide Google, Inc. (Nov. 8, 2017), https://support.google.com/webmasters/answer/7451184?hl=en (last visited Nov. 8, 2018).

NTIA should hold ISP's accountable and transparent and emphasize notice, choice, consent and privacy by design. In the process, the NTIA can push privacy forward.

Respectfully,

C. Kaysen