

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
Washington, DC 20230
Attention: Privacy RFC

Re: Docket No. 180821780-8780-01 Developing the
Administration's Approach to Consumer Privacy

Dear National Telecommunications and Information Administration,

Thank you for the opportunity to comment on the National Telecommunication and Information Administration's approach to consumer privacy. As a law student in an Information and Data Privacy course, an in-house legal extern for a multi-billion dollar corporation, a daughter of small business owners and a millennial consumer, I am excited to contribute my multi-faceted insight to the efforts in modernizing the U.S. data privacy policy for the 21st century.

The most powerful commodity in the post-modern era we live in *is* information. Unlike the eras before us, in which people and organizations capitalized on things like gold and oil, in this information era, the objects of value are not objects at all. Rather, they are the intangibles of *data*. What size shoe do you wear, where do you live, what websites do you visit, what are your interests? These are all types of valuable data that is being collected, analyzed, and sold today - often without the consumer's knowledge or understanding. As the value of information skyrockets, due to advanced algorithms and technology, so do the aggressive efforts by companies and organizations to continue to collect and analyze this data to gain prosperity and achieve innovation. The need for legal ground-rules surrounding innovation and use of consumer information is as great as ever.

In working towards a solution, this Administration is focused on the positive outcomes of organizational practices designed to protect consumer data, rather than on dictating what those practices should be. This begs the question: How can organizations be induced to do what is best for the consumer without specific guidelines on what actions to take? Treat data collectors as fiduciaries of consumers' personal data. A fiduciary is a person or entity that has an obligation to act in a trustworthy manner in regard to the collection, analysis, use, and disclosure of their client's information. Like traditional fiduciary roles, data collecting companies have relationships with their consumers that involve an imbalance of power, an undertaking, trust, and vulnerability. Therefore, sensibly, treating data-collecting organizations as fiduciaries of consumers' personal data would accomplish all of the administration's goals.

I. What is a Fiduciary?

A fiduciary is a person or entity that has an obligation to act in a trustworthy manner in regard to the collection, analysis, use, and disclosure of their client's information. Scholars have suggested that professionals given duties with respect to personal information obtained in the course of their relationships with their clients should be considered a special type called an "Information Fiduciary".¹ The law has recognized the role of fiduciaries for over 250 years.² The concept arose from the existence of asymmetrical power in economic relationships, such as when ordinary people entrust their personal information to skilled professionals like accountants, investment analysts, doctors, and lawyers. In exchange for this trust, such professionals undertake a duty of loyalty and a duty of care to their clients. Under a duty of loyalty, fiduciaries

¹ Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1208 (2016)

² *Keech v. Sanford*, 25 Eng. Rep. 223 (1726).

cannot use their clients' information against their clients' interests.³ Under a duty of care, fiduciaries must act competently and diligently to avoid harm to their clients.⁴

Attorneys are examples of information fiduciaries. They have unique access to their clients' personal information, and a unique ethical obligation to use that sensitive information only in the best interests of their clients. But, where there is power there is often exploitation. The Professional Rules of Responsibility ("the Rules") address this vulnerability and seek to ensure that attorneys do not wield their power of client-information in any harmful way. Of course, a client could just as easily be harmed by her attorney using her personal information against her, as she could by her attorney carelessly or recklessly guarding that personal information. And so the Professional Rules of Responsibility address both instances of active use of a client's information against her, and omissions or failures that subject the client to a leak of her personal information. For example, the Rules prohibit an attorney from using information about a previous client to later harm that client when the attorney represents someone new who is adverse to the previous client.⁵ And, the Rules also prohibit an attorney from revealing her client's confidential information to anyone without the client's permission.⁶

II. Data Collecting Organizations Act As Fiduciaries

Internet and technology companies that harvest and monetize their consumers' personal data should be treated as fiduciaries for the same reasons accountants, investment analysts, doctors, and lawyers are. Ari Ezra Waldman, an internationally sought-after scholar of data privacy, writes "rather than limiting corporate responsibility to giving us a list of data use

³ Restatement (Third) of Agency § 8.01 (2006)

⁴ Restatement (Third) of Agency § 8.08 (2006)

⁵ Model Rules of Professional Conduct Rule 1.9(a)

⁶ Model Rules of Professional Conduct Rule 1.6(a)

practices for rational privacy decision-making, privacy-as-trust recognizes that data collectors are being entrusted with our information. They are, in fact, fiduciaries with respect to our data, and should be obligated to act in a trustworthy manner.”⁷ Congruent to typical fiduciary relationships, the relationship between consumers and internet and technology companies involve an imbalance of power, an undertaking, trust, and vulnerability.⁸

First, there is, undoubtedly, an imbalance of power. These companies possess skills ordinary consumers do not have, access, analyze and process data in ways consumers could not fathom and create algorithms that will never be revealed to consumers due to trade secrecy.⁹ On top of this, consumers are incredibly dependent on these internet and technology companies as it is absolutely impossible to engage in modern life without the Internet.¹⁰ Information is power and companies know and have more information about how their services and consumers work than the consumers themselves.

Second, Internet and technology companies undertake the role as service providers for the interests of consumers. A fiduciary relationship will often arise when one person undertakes to act in the interests of another.¹¹ These companies market themselves as experts in the services they provide in exchange for consumers’ personal information.¹² Facebook is the best and largest social connector¹³, Match.com calls itself “#1 in dates, relationships, and marriages,”¹⁴ and

⁷ Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age 85* (Cambridge University Press 2018).

⁸ AJ Oakley *Constructive Trusts* 3rd ed, Sweet & Maxwell, London, 1997 at 90-98.

⁹ Waldman, *supra* note 5 at 86.

¹⁰ *Id.*

¹¹ Austin Scott, *The Fiduciary Principle*, 37 Calif. L. Rev. 539, 540 (1949).

¹² Balkin, *supra* note 1 at 1222.

¹³ See Waldman *supra* note 5 citing Mark Zuckerberg, Facebook (Aug. 20, 2013), www.facebook.com/zuck/posts/10100933624710391.

¹⁴ See Waldman *supra* note 5 citing Match, www.match.com/cpx/en-us/match/IndexPage (last visited Nov. 08, 2018).

Google is the dominant search engine and primary avenue to the World Wide Web for most Internet users.¹⁵

Third, companies hold themselves out as trustworthy.¹⁶ These Internet and technology companies know that in order to use their services, we must give them our personal information. Because this personal data is so valuable, companies hold themselves out as trustworthy organizations who act consistent with our interests, while hoping to make a profit.¹⁷ Facebook published a set of “Community Standards” to inform users of the many ways the platform creates a safe online environment for users.¹⁸

Fourth, the asymmetries stated above place consumers in a significantly vulnerable position when using company services. We place our personal information, our money, our health, and our fate in their hands.¹⁹

III. The Fiduciary’s Role Satisfies the Administration’s Goals

The core of a fiduciary’s role are the heightened duties they are required to serve. A fiduciary holds a duty of loyalty and a duty of care to their interested parties. The practical effects of these duties satisfy each of the Administration’s goals.

Under a duty of loyalty, fiduciaries cannot use their clients’ information against their clients’ interests.²⁰ This duty alone achieves the administration’s goals of *transparency, control, and access and correction*.

¹⁵ See Waldman *supra* note 5 citing Dan Frommer, *Google Has Run Away with the Web Search Market and Almost No One Is Chasing*, Quartz (July 25, 2014), <http://qz.com/239332/google-has-run-away-with-the-web-search-market-and-almost-no-one-is-chasing>.

¹⁶ Waldman *supra* note 5.

¹⁷ Balkin *supra* note 1 at 1222.

¹⁸ Facebook, *Community Standards*, <https://www.facebook.com/communitystandards/> (last visited Nov. 08, 2018).

¹⁹ Balkin *supra* note 1 at 1216-17.

²⁰ See *supra* note 3.

A. Transparency

Transparency is achieved because by default, consumers understand that data collectors as fiduciaries, cannot use their clients' information against their clients' interest. While this does not solve the imbalance of power due to trade secrecy, the consumer knows the collection, storage, usage, and sharing is for the consumer's particular interest and entrusts that as a fiduciary, the data-collecting entity will *only* collect, store, use, and share their information for that interest. To ensure that companies are not using their clients' information against their interests, companies would take into account how the average user interacts with the companies' products or services. Understanding the purpose behind consumers' use of and interactions with the products or services and serving *only* towards that use and interaction shows consumers that the company is collecting, storing, using, and sharing the personal information for the particular client's interest. For example, perhaps I want to get a monthly magazine subscription. If I were to give Conde Nast my personal information to sign up for a magazine subscription of Conde Nast Traveler, I understand that Conde Nast, as the fiduciary, would collect, store, use, and share my data for the purpose of getting my magazine subscription. Conde Nast owes me a duty of loyalty to use my information for my interest of getting the magazine subscription. If Conde Nast shares my information with Jet Blue and I start receiving e-mails on flight deals to tropical destinations, Conde Nast would be acting against my interest. My sole interest in Conde Nast was to receive their subscription. Conde Nast has shared my information against what is reasonably necessary to serve my interest of getting their magazine subscription and did not ask for my consent to share my information beyond my interest. Here, Conde Nast has acted against transparency and has breached their duty of loyalty to me. Transparency gives the consumers

trust and confidence because consumers know the purpose of the collection, use, storage, and disclosure of their information. This kind of transparency in a fiduciary relationship protects innovation on behalf of companies because consumers do not need to know the specific formulas and algorithms used to serve their interests, but just that their interests are served and nothing beyond.

B. Control

Companies as fiduciaries are required to be loyal to their consumers meaning, fiduciaries are *controlled* by their clients. A consumer has reasonable *control* over the collection, use, storage, and disclosure of their personal information because consumers control the purpose for what that information is collected, used, stored, and disclosed for. The company, as a fiduciary, must abide by the consumer's decision on what to do with their personal information. Even in traditional fiduciary professions, which controls to offer, when to offer them, and how they are offered depend on context. In an attorney-client relationship, the client control the goals of the representation which specifically requires that the lawyer abide by the client's decision whether to settle a matter, and in criminal cases whether to plead guilty, waive, a jury trial, or testify.²¹ Depending on the companies' services and the differing purposes consumers are engaged with these companies, *control* is flexible and cannot be spelled out. But what remains constant in a fiduciary relationship, is that consumers' control can be used to withdraw consent and to limit the activity previously permitted just as accessible as they were permitted. In this case, innovation is not affected because innovation of the service has already been established. Companies should not fear that their innovation will fail if users decide not to provide certain

²¹ Model Rules of Professional Conduct 1.2(a).

sensitive personal information that is needed for the service or product to work. Consumers are more willing to give their information to a service because that information is reasonably necessary for a specific purpose. If I want to use a budgeting app to manage my finances, I am more inclined to give the app my bank information versus giving Facebook my bank information. Trust and confidence in a consumer's relationship with an internet and technology company is solidified because the consumer has reasonable control over their personal information.

C. Access and Correction

Naturally, with control in a fiduciary relationship, consumers would have *access and correction* to their personal data. Consumers would be able to access their personal data to rectify, complete, amend or delete this data. Fiduciaries are at the service of their clients, and to better serve them, fiduciaries would welcome their clients access and correct this data. This would not only build trust and confidence in the relationship but also better cater the innovation towards the client.

Under a duty of care, fiduciaries must act competently and diligently to avoid harm to their clients.²² This means that internet and technology companies, as a fiduciary, would take care to eliminate avoidable risk through *reasonable minimization, security, and risk management*.

D. Reasonable Minimization, Security, and Risk Management

²² See *supra* note 4.

Companies would ensure that the collection, storage length, use, and sharing of data is *reasonably minimized* to the interest of the consumer and the company. This means companies should collect information that is reasonably needed. Facebook would not need bank information, but a financing app would. Since companies are entrusted with our personal information, it is within their duty to take care of it by employing *security* safeguards to secure this data at all stages. By nature of the fiduciary relationship, consumers expect that their data would be protected from loss and unauthorized access, destruction, use, modification, and disclosure. By taking these actions to collect, store, use, and share data reasonably necessary and by providing security safeguards, companies are in effect practicing *risk management*. Innovation can still prosper as long as organizations take care to prevent consumer harm and maximize privacy outcomes.

Ultimately, identifying data collecting organizations as fiduciaries accomplishes *accountability, incentivizes privacy research, encourages harmonization and interoperability, has comprehensive application, provides legal clarity while maintaining the flexibility to innovate, employs a risk and outcome-based approach, is scalable* and can be enforced by the *FTC*.

E. Accountability

By nature of the fiduciary role, internet and technology companies collecting data are *accountable* through their duty of loyalty and duty of care to their consumers. Companies recognizing their fiduciary duty will want to be proactive and incentive “privacy-by-design” as their best tool to achieve their privacy outcomes of transparency, control, access and correction, reasonable minimization, security, and risk management. As a fiduciary of our data, these

companies would take steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data.

F. Incentivize Privacy Research

Rather than thrusting internet and technology companies to their financial demise from developing products and services through trial and error, or waiting for the largest data breach to unfold to make an example of, the government should *incentivize prioritize research*. The research into and development of products and services that improve privacy protections will aid in ensuring that privacy in innovation is attainable and that privacy in innovation is important. Companies would also not be chilled or turned off from employing privacy tools, because the government would have already researched or developed the privacy tools.

G. Harmonization of the Regulatory Landscape and Interoperability

Considering data collecting organizations as fiduciaries of our information will encourage *harmonization of the regulatory landscape and interoperability* because the concept of the role is familiar. The concept of a fiduciary has been around for over 2 centuries and ordinary people interact with fiduciaries all the time and are familiar with their roles. The concept would be easily adapted and understood throughout the regulatory landscape as consumers would think data collectors serve and are responsible to them just as their doctor, lawyer, accountant, and investment analyst are. A breach of the peace would not occur by simply acknowledging what consumers already feel about data collectors, that they are fiduciaries entrusted with our personal information.

H. Comprehensive Application

In addition, the concept of the fiduciary relationship has *comprehensive application*. A fiduciary relationship takes a trust-based approach. The duties and obligations required of fiduciaries in handling our personal data is flexible to apply in both the private and public sector.

I. Legal Clarity While Maintaining the Flexibility to Innovate

Recognizing internet and technology companies that collect our personal data as fiduciaries would provide *legal clarity while maintaining the flexibility to innovate*. Organizations have clear rules to fulfill their duty of loyalty and duty of care to their consumers yet organizations still have the flexibility for novel business models and technologies, as well as the means to use a variety of methods to achieve consumer-privacy outcomes.

J. Employ a Risk and Outcome-Based Approach

Fiduciaries *employ a risk and outcome-based approach*. Fiduciaries undertake a role to serve the interests of their clients. In handling their client's personal information, fiduciaries are focused on user-centric privacy outcomes. The role of the fiduciary in regard with personal information is naturally flexible to balance business needs, consumer expectations, legal obligations, and potential privacy harms.

K. Scalability

The concept of the fiduciary role is *scalable* and can be applied to small businesses that collect little personal information about their customers. As a fiduciary, a small business owner is still required to make good-faith efforts to utilize privacy protections. Fiduciary relationships

and the duties required of them vary in different context due to the quantity and quality of personal information collected. The distinctions between organizations that control personal data and third-party vendors that merely process that personal data on behalf of other organizations have different duties and expectations due to the purposes for which the personal information is collected, used, stored, and disclosed.

L. FTC Enforcement

Lastly, *FTC Enforcement* is viable and within the scope of the federal agency's jurisdiction as data collectors should be considered information fiduciaries. Because this is not a new concept, the FTC has a leg up on having the necessary resources, clear statutory authority, and direction to enforce consumer privacy laws in a manner that balances the need for strong consumer protections, legal clarity for organizations, and the flexibility to innovate.

IV. Conclusion

The administration should rethink data collecting organizations as information fiduciaries. A fiduciary is a person or entity that has an obligation to act in a trustworthy manner in regard to the collection, analysis, use, and disclosure of their client's information. Like traditional fiduciary professions, data collecting companies have relationships with their consumers that involve an imbalance of power, an undertaking, trust, and vulnerability.²³ The practical effects inducing companies to serve consumers' interests stem from the duty of loyalty and duty of care. Sensibly treating data-collecting organizations as fiduciaries of consumers'

²³ Oakley *supra* note 8.

personal data would accomplish all of the administration's goals, thereby protecting consumer privacy while fostering innovation and prosperity.

Sincerely,

Katarina Sykes