From: Jeff Murnane
To: privacyrfc2018
Subject: Comment on Docket No. 180821780-8780-01
Date: Tuesday, October 23, 2018 9:47:46 AM

As an entrepreneur that left a steady income to start my own, data-based technology company over 10 years ago, personal data rights is something I've been very passionate about. I truly believe that there are few things as important to our technological future than an individual's data rights, which are as important today and in the future as property rights have been since the founding of our country. The US constitution which established the foundation for these property protections later codified under U.S. law recognized the importance of personal property, but could not have predicted the digital age in which we live in today. As a strong supporter of these rights I welcome the opportunity to respond and offer comment to this very important issue of data rights that face Americans today.

I believe that the Internet as it exists today, with massive cloud-based data repositories controlled by a few large companies, is fundamentally incapable of transitioning to an owner-centric foundation for data rights, or even provide adequate security around data. The organizations that currently control our data would have to relinquish the very financial incentives that have fueled their massive online advertising-based revenue growth across the web for years, is at fundamental odds with the data security interests of individual data owners.

An unfortunate by-product of the monumental shift to digital commerce created by the internet, is the loss of individual privacy and security rights of the consumer. Because the Internet grew rapidly and organically with little preconceived direction or centralized structure, and due to the prevalence of advertising-based revenue models based on personal web browsing data, privacy concerns around personal data became an afterthought. At the same time, search engines and social networks grew to dominate Internet usage, with increasing power going to a relatively few companies which grew massively by giving away services for free, but using the personal data of its users to, in turn, monetize their platforms via advertisers.

Simultaneously, the ability of cyber criminals and hostile governments to exploit the lack of adequate security around data via various nefarious methods and/or security flaws in platforms and software has given rise to the massive data breaches that occur almost daily. As a result, individuals have become virtually powerless to protect their personal information including their identity and even life savings, from cyber-theft or compromise.

This must change, and fast. Customer data collected by organizations has thus far been considered the property of the collector and not the individual, where it rightfully belongs. Along with this data collection practice has been abuse of this data. While privacy policies around personal data have grown more comprehensive, they are not consistent from business to business. They are often written as legal contracts and are too complex for the average person to understand, and in most cases are created for the benefit of the business, and not the individual.

Companies over time have also collected more and more customer data to generate more and more revenue, and online activity monitoring became prolific thanks to companies like Google and Facebook. It wasn't good enough to just know which websites customers came from and left for, all online activity could now be tracked and monetized into more pervasive targeted advertising. Individuals and their data are now being treated as a corporate commodity, to be traded, exploited and monetized by 3rd parties, ostensibly in return for "a better online experience." Nowhere does compensation to the actual data owners themselves enter the picture.

Ultimately the entity who pays when their data isn't protected and falls into the wrong hands is the individual consumer. He or she pays in the form of identity theft, hacked accounts, bank fraud, unwanted advertisements and the list goes on. Lives have been destroyed and life savings drained due to the vulnerability and/or carelessness of organizations that have been trusted to be the caretakers of customer data.

I, along with countless others, understand that technology has advanced to the point today where individuals and their data can be better protected, as well as be leveraged to facilitate a systemic shift in how data is treated. Advancements in distributed ledger technology such as Blockchain offer creative solutions to the many existing problems with data today, especially when combined with advanced encryption technology and leveraging public and private keys for data access. A blockchain or blockchain-like solution would offer an immutable data record, verified through scalable distributed ledger and encryption technology, offering far better data security at the data owner level vs. today's more centralized "big data" clouds. Most importantly, such a solution would offer data interoperability, enabling businesses across disparate industries to collaborate around customer data of common interest.

The key to such data interoperability is placing the data controls in the hands of the data owners which are primarily, though not exclusively, individual consumers. Information about an individual should be considered property of that individual. Collectively, individuals have a right to not only know what a company has collected about them, but to also control access of that information. With transparency around and the controls to access personal data, entities can gather data from the source, significantly reducing the expense and complication of "big data" collection and validation. Consumers become incentivized and much more savvy about their own information, and take on the heavy lifting of updating and verifying their own data. Data quality improves substantially, the ethical use of data increases, while unethical use cases such as "fake news," bots, and data fraud, decrease. Of key importance, opportunities and incentives to monetize personal data shifts from the current Googles, Facebooks and Amazons of the world to the real data owners, individual consumers.

With individual data owners responsible for granting permission to access their data, business incentives also change. Organizations will need to rethink how customer data is used in a permission-based world and still have the flexibility to balance business needs and legal obligations with customer expectations. Access to consumer data transforms from an expensive liability into a revenue generating opportunity for all data owners, not just the Googles of the world. This levels the playing field for all individuals and businesses and promotes creativity, innovation and better customer service. Data waste in the current system (incorrect or discrepant data) is reduced significantly, and the entire online marketing structure is disrupted in favor of individual data owners. With consumers in control, data can be exposed to appropriate marketers at the appropriate time of the owner's choosing. Combined with more accurate consumer financial data curated by its owner, and the lopsided business-to-consumer marketing relationship of today is replaced with a more equal connection on a more equal footing resulting in a mutually beneficial relationship.

Government's Role

Government can and should play a vital role in this transformation in several key ways. First, government should enact and enforce "individual data rights" legislation that unequivocally grants individual persons and organizations the right to privacy and ownership of their personal data, and clears a path for the private sector to respond with new technologies, platforms and services. This can be accomplished first by establishing a new unique, personal identifier for U.S. citizens to replace the limitations and drawbacks of the Social Security Number. This first step would eliminate SSN-related identity theft and be the first big step in protecting American citizens' individual data rights.

Second, government will need to set the rules to ensure a level playing field. Federal and state legislation should be considered that provides a legal framework establishing enforceable data rights for data owners, and enabling the private sector to innovate around providing better data security and the ability for data owners to monetize personal data. Government can also prevent monopolistic behaviors by enforcing anti-trust laws and assure that data sharing and technologies that facilitate it remain open to all owners and consumers of data, versus picking winners.

Lastly, the U.S. government should focus on protecting U.S. citizens' data rights internationally. This can be accomplished through a combination of multi- and bi-lateral agreements, treaties and trade pacts, as well as cyber security monitoring and defensive counter measures against large-scale cyber-attacks.

Ultimately, the US government has a responsibility today to protect its citizens and their property rights, which today includes digital personal data, and enact and strongly enforce legislation that clears the path for free enterprise and innovation to flourish.

Jeff Murnane

Omaha Nebraska