March 15, 2019

Comments of Digital Liberty

Question 5: What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

Dear Chairman Crapo and Ranking Member Brown:

Thank you for the opportunity to provide comments on consumer data privacy. This comment suggests a method that could be used to address consumer data that is neither sensitive nor public, but perhaps falls into another category.

The market for user data is a relatively new marketplace where individuals are affected by a company's practices, but those individuals are not the company's customers. Because the user is not the customer, companies may not be entirely responsive to the requests or needs of their users in the same way that they are responsive to their customers. The following ideas could offer a targeted mechanism to promote privacy principles in the marketplace.

There is a distinction between companies that sell products to users and companies that sell user data or advertising to users.

Within this context, guidance for another category of personal data – user-controlled data – could be helpful. For example, activities that fall into the user-controlled category should not be tracked across websites or platforms without the user's consent and no functionality should be lost if a user determines they do not wish to be tracked.

The user-controlled category should still allow for business models that would offer users reduced monetary expenses, received payments, or like kind exchanges for their valuable personal data.

There are many ways to explore the concept of user-controlled data. Some activities that could be included, but not limited to this category, might be: search, browsing, and viewing/listening habits. The user-controlled category falls in between non-sensitive and sensitive user data. It is data that is not about the user, but about the user's aggregated habits. This type of data likely does not fall into the category of requiring breach notification, but the user should have a level of decision-making power over its collection, thus user controlled.

However, there is a difference between using live-time consumer data for the functionality of a service or device, versus tracking or storing data for other purposes outside the functioning of the device or particular product experience.

By using a website, App, or platform a user is sharing their data and habits with that company, and that **company should be able to use data obtained within their own universe to enhance products and services**, but once a user leaves that platform, they should be able to do so without being tracked.

For example, a Search Engine or Browser knows what was searched for and what link was clicked on, but it does not need to retain knowledge of how the user interacted with the page visited or how long the user was on the page.

To further illustrate, while using an Online Marketplace or Streaming Service, the Marketplace and/or Streaming Service has data on a user's shopping, viewing, and/or listening habits that are shared by virtue of using the service. The Marketplace or Streaming Service should be able to use that data to enhance user experience on the platform, for example product recommendations; however, when a user leaves the website, tracking should not continue without user consent.

To take the example a step further, if the user visited a Marketplace or Streaming Service through a Search Engine or Browser, the Search Engine or Browser should not be following all that the user is doing on other websites unless the user consented to such exchanges. This should also apply to the infrastructure these services operate through.

By using a service, operating system, software, or device a user is sharing their data and habits with that company, but the company should not be able to track the user within other services, operating systems, software, or devices that the initial implement allowed the user to access.

This concept is illustrated through the relationship between mobile devices and Apps. The act of using the device and operating system of the phone, should not equate to the relinquishment of all control over a user's data. When entering an App the data should be confined to that App and not communicated with the operating system and used without consent.

While there is a difference between companies that sell products to users and companies that sell user data, the concept of user-controlled data does not need to be sector specific. **These ideas on user-controlled data translate to certain interactions taking place around the traditional business-customer relationship when there is a data exchange**. For example, data gathered via customer loyalty cards and apps, or through interaction with a device such as a motor vehicle or other machine that also collects/analyzes data.

I am happy to discuss these ideas further or answer any questions you may have.

Regards,

Katie McAuliffe
Executive Director
Digital Liberty