“Right to be forgotten” or “right to erasure” is an element in both European Union’s General Data Privacy Regulation and regulations in Canada. Consumers generally have no effective way to understand or control what happens with the data an entity collects, where their data goes, how long the data is stored, and to whom the data is sold or shared. Often this is sensitive information, including location data, children’s data, and other sensitive personal information. The right to erasure allows the consumer to ask the data-gathering company to delete what data they have on that particular consumer. Typically the right has sideboards of how the consumer must share the request, and who may ask for information to be deleted.

In order to be meaningful, data should be easy to access and erasure should be at no extra cost to the consumer. The “right to be forgotten” would be beneficial to consumer privacy, but also data security. If an entity is responsible for deleting data, then the entity may be motivated to collect only the data that is needed as part of the function of the service or product. This concept of data minimization is a simple way for entities to prevent the burden of storing, accessing, tracking, and ultimately deleting data. In other words, the less an entity collects and stores, the less the entity will need to spend on compliance for the right of erasure.

In the autonomous vehicle context, the right to be forgotten could be especially important in several scenarios: in transfer of ownership of a vehicle, location data, ride data from a transportation network company, and in many other contexts.

The right to be forgotten will need to be balanced with competing concerns for the retention of data: public records law compliance (if shared with a government agency), subpoenas and other legal compliance concerns.