PRIVACY CONSIDERATIONS

Synopsis of the issue

Data privacy is a concern to many individuals. Well-known examples of events that lead to this concern include the 2017 Equifax data breach[1] and the Facebook and Cambridge Analytica scandal, which led to a 66 percent decline in trust among surveyed Facebook users that the social media site was committed to protecting the privacy of their personal information.[2] This, along with other recent data breaches, may have customer trust repercussions for years to come. Consequently, policymakers and automakers have an interest in ensuring that they keep riders' private information secure.

In a transportation context, personally identifiable information is defined as unique data that carries the potential of being used to identify a single individual. Examples of personally identifiable information include full name, telephone number, street address, email address, email password, vehicle registration plate number, driver's license number, credit card numbers, and one's digital identity (Douma & Deckenbach, 2009, pp. 318-319). More specifically, personally identifiable *location* information (PILI) is considered data that could be used to identify an individual (e.g., license plate number) as being at a particular location at a particular time (Garry, Douma, & Simon, 2012, p. 106). Tolling transponders that gather information about the movement of a vehicle on a stretch of road to collect use revenue fall into this category (Douma & Aue, 2011, p. 15). Conversely, anonymous locational information, or non-PILI, cannot be tied back to a specific individual. Examples include information from traffic counters or devices that only detect the presence of vehicles in order to control traffic flows, without identifying the vehicle (Douma & Deckenbach, 2009, pp. 318-319).

These general concerns, along with the general perception that payment of distance-based fees (DBFs) would require government tracking of the location of individual vehicles, and, by extension, the occupants of those vehicles (Congressional Budget Office, 2001), protecting the privacy of PILI is a significant legal (and business) issue. Consequently, it is worth exploring the actual legal landscape to help understand what locational data is protected and what is not, so that those implementing DBF are able to clearly address these concerns when raised by members of the public.

---

[1] "Equifax to pay up to $700M in data breach settlement," KARE 11, July 22, 2109. Available at https://www.kare11.com/article/news/nation-world/equifax-to-pay-up-to-600m-in-data-breach-settlement/507-9c9dd21d-b7aa-4d41-8d5f-92e5bfff2621, last accessed March 13, 2020

[2] Weisbaum, H. (2018, April). Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal. CBS News. Retrieved from https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011

Sources of Privacy Protection

Federal Constitutional Protections

The United States Constitution, specifically Supreme Court case law on the Fourth, Ninth, and Fourteenth Amendments, is a core source of American privacy law. With respect to the transportation context, case law on the Fourth Amendment is the most relevant and has become more protective of privacy as technology has evolved.

- The basic test for whether a person has a protected privacy interest under the Fourth Amendment comes from the 1967 U.S. Supreme Court case, *Katz v. United States*[3]. Under *Katz,* a reasonable expectation of privacy exists when: (i) a person has an expectation of privacy, and (ii) society deems the expectation to be reasonable.
- Regarding protection of one's location on the road, the Court initially interpreted the "societal expectation" prong of the Katz test to mean that privacy protections did not apply. In a 1983 case, *United States v. Knotts*, the Supreme Court stated, "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[4]
- Rapid technological change, however, may be leading the Court to change this interpretation. In 2010, the Court noted that technology was evolving so rapidly that it was almost impossible for a court to determine the corresponding societal expectation of privacy.[5] Then in 2012, the Court decided a case involving GPS tracking using an analysis framework other than the *Katz* test, though without necessarily rejecting the primacy of *Katz.*[6]
- Two years later, in 2014, the Court indicated a new understanding of "societal expectations. In *Riley v. California*, the Court determined that searching through a cell phone without a warrant was a violation of 4th amendment rights, characterizing cellphones as "minicomputers" filled with massive amounts of private information.[7] The Court's use of the term "minicomputers" left this ruling open to application to a range of technologies—potentially including fleet service applications that store passengers' information.
- Finally, in a 2018 case, *Carpenter v. United States* (2018), the Court held that the government needs a warrant to access a person's cellphone location history.[8] Although the case addressed cellphone location data, the majority made it clear that the ruling applies to "information that can locate people generally, not just [cellphone location data] specifically."[9]

---

[3] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[4] United States v. Knotts, 460 U.S. 276, 281 (1983).
[5] City of Ontario v. Quon, 130 S. Ct. 2619, 2629-30 (2010)
[6] United States v. Jones, 132 S. Ct. 945, 950-53 (2012).
[7] Riley v. California, 573 U.S. 373 (U.S. 2014)
[8] Carpenter v. United States, 138 U.S. 2206 (U.S. 2018)
[9] Ohm, P. (2018, June). The broad reach of Carpenter v. United States. *Just Security*. Retrieved from https://www.justsecurity.org/58520/broad-reach-carpenter-v-united-states/

Looking at the changing interpretations of "societal expectations" related to what data is private as technologies allow increasing amounts of data to be collected and stored, it appears to be possible that PILI data collected as part of a DBUF project may be private. However, without a direct ruling stating this, additional measures may be prudent.

Federal Law

Several existing federal laws create privacy protections, albeit in relatively discrete areas (Douma & Deckenbach, 2009, p. 303). Very few of these laws have direct relevance for distance-based user fees. Among those that might, the most relevant are the *Driver's Privacy Protection Act of 1994,* which protects personal information collected by departments of motor vehicles, and *the Privacy Act of 1974,* which regulates how the federal government handles the personally identifiable information it collects.[10] In addition, the Federal Trade Commission, under Section ***5*** of the *Federal Trade Commission Act,* has become active in regulating companies' privacy notices to consumers about how they collect and use consumer data, including locational data.[11]

State Law[12]

Federal law sets the floor of privacy protection upon which States have the ability to build their own privacy regulations. As a result, the extent to which privacy is protected beyond the federal level varies across states. Some state courts have interpreted their state constitutions in a way that expands the privacy rights of their citizens beyond those prescribed by federal constitution. Similarly, some states statutorily extend privacy protections beyond those afforded by federal law. But like federal law, state statutes generally approach privacy in a piecemeal, area-by-area fashion.

There are not many state laws specifically addressing privacy and transportation technologies. Most laws only address specific technologies whose use is either controversial with the public, such as automated speed enforcement, or where there is a perceived potential for abuse. State privacy torts, such as intrusion upon solitude, public disclosure of private facts, "false light" publicity, and misappropriation of likeness, provide an additional source of privacy protection. However, these torts do not usually create a cause of action on public streets and have not yet been successfully applied in any cases involving tolling or other ITS technologies.[13]

[10] Driver's Privacy Protection Act of 1994, 18 U.S.C. H§ 2721-2725 (2011); Privacy Act of 1974, 5 U.S.C. § 552a (2011).
[11] Federal Trade Commission Act, 15 U.S.C. § 45(a) (2011) (prohibiting unfair or deceptive acts or practices in or affecting commerce).
[12] This section draws on Douma & Deckenbach, 2009, pp. 307-310
[13] See, e.g., Kendra Roseberg, Location Surveillance By GPS: Balancing an Employer's Business Interest with Employee Privacy, 6 WASH J.L. TECII. & ARTS 143, 150-54 (2010).

Implications of Privacy Law for Distance-Based Fees

The tangled and unsettled nature of privacy law in the U.S. means its application to Distance-Based Fees is often jurisdiction, technology, and context-specific. Nevertheless, several principles can be stated: [14]

- The less personally identifiable the information collected; the fewer privacy issues will arise. When the data collected does include personally identifiable information, however, legal issues regarding consent, access, ownership, and protection of information are often triggered.
- When an ITS application collects personally identifiable information about an individual, consent to obtain that data generally should be obtained from that individual. Voluntary consent ("opt-in") is one way in which consent can be given. Voluntary consent generally requires individuals to manifest willingness to have their personal information collected, and they must be informed of some specific aspects of the information being collected. The other form of consent is to imply consent (opt-out). Courts have found implied consent to be sufficient when the government's interests in preventing injury, property damage, and loss of life on roadways are served by the practice. However, presumed or implied consent usually must allow for individuals to opt-out of such programs and requires that members of the public be made reasonably aware of what they are tacitly consenting to.[15]
- Current law typically places much greater restrictions on the collection and use of personally identifiable data by the public sector, than by the private sector.38 Thus, who is collecting and/or using the information gathered by an ITS application often dictates the level of privacy protections triggered.

As noted above, if the data is collected by the State or other public entity, there may be legitimate legal privacy concerns as there are few protections against a person's location, unless specifically provided by a state statute.

If participation in a Distance-Based Fee program is voluntary (i.e. "opt-in") the expectation of privacy is diminished significantly. The association of a toll transponder to a vehicle or vehicles instead of a person also creates some anonymity, is a secondary protection regarding legal privacy; travel history details only provide information about the location of the transponder, not about a specific individual.[16]

Similarly, if the data is collected by a private entity rather than the state, then protection is likely further increased. Private entities can restrict data sharing to ways they define through their own privacy policies, to which customers consent to when they enroll. Secondly, these entities can limit the data they share with the state to aggregate data that does not include individual information.

---

[14] These principles come from Douma & Deckenbach, 2009, pp. 318-321 except as otherwise noted
[15] This issue was covered in more depth in a report on online privacy (U.S. Department of Commerce Internet Policy Task Force, 2010).
[16] This case is discussed in greater detail in Douma & Aue, 2011, p. 16.

Demonstrations are incorporating these practices to address these privacy concerns. For example, the Reason Foundation analysis of Oregon's demonstration noted that "The state of Oregon's permanent MBUF program uses a one-way system and third-party data collection to keep personal driver data confidential. The state does not have access to a driver's location" (Smet & Feigenbaum, 2019). Similarly, Minnesota's 2011 Mileage-Based User Fee Policy Task Force pointed out that privacy can be addressed in the following ways:

- Not collecting the data through use of pre-paid debit cards
- Limiting data collection through:
- Anonymous user accounts that do not disclose the vehicle ID
- Only collecting odometer readings
- Retaining data in the vehicle (no transmission except for the fee charged)
- Limiting data retention by immediately deleting data after the mileage fee is determined
- Limiting data access by contracting responsibility to a third-party, non-governmental entity
- Protecting the data through sophisticated data encryption[17]

[17] Other relevant works include the technical report Munnich, Doan, & Schmit (2011) and Munnich, Robinson, & Zhao (2011).

WORKS CITED

Congressional Budget Office. (2001). *Alternative Approaches to Funding Highways.* Congressional Budget Office.

Douma, F., & Aue, S. (2011). *ITS and Locational Privacy: Suggestions for Peaceful Coexistence.* Retrieved from the University of Minnesota Digital Conservancy. Minneapolis, MN: University of Minnesota Center for Transportation Studies.

Douma, F., & Deckenbach, J. (2009). The Challenge of ITS for the Law of Privacy. *University of Illinois Journal of Law, Technology & Policy, 2*, 295.

Garry, T., Douma, F., & Simon, S. (2012). Intelligent Transportation Systems: Personal Data Needs and Privacy Law. *Transportation Law Journal, 39*(3), 97.

Smet, P., & Feigenbaum, B. (2019). *Mileage-Based User Fees Represent a Sustainable Way to Pay for Highways.* Reason Fundation.

U.S. Department of Commerce Internet Policy Task Force. (2010). *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework.* U.S. Department of Commerce.