Data Privacy, Security, and Consumer Protection

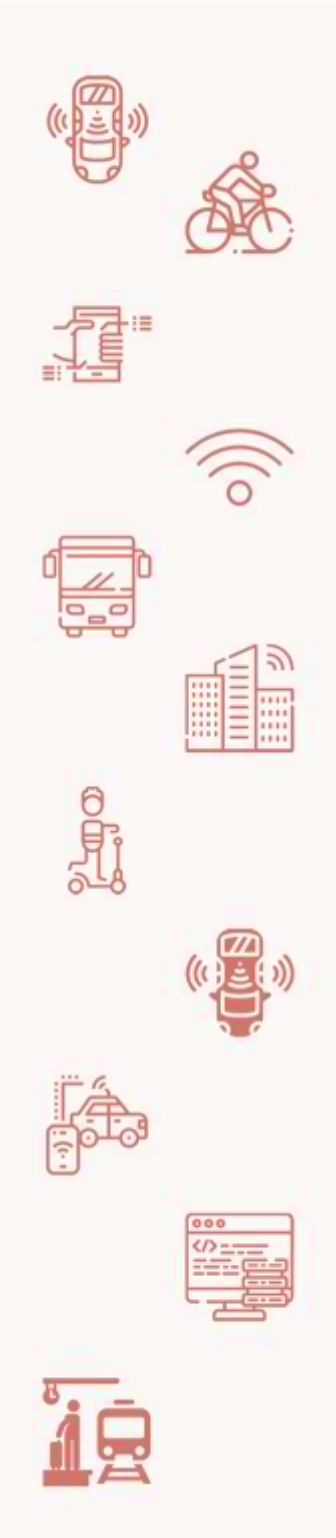
White Paper

How can Texas agencies improve data privacy and security practices in order to protect consumers and save resources?

In March and April 2020, governments and health organizations all over the world scrambled to inform and protect their citizens and patients as the novel coronavirus, COVID-19, swept across the globe. Some federal governments in countries such as South Korea, Italy and Israel elected to harness technologies such as surveillance-camera footage, smartphone location data and credit card purchase records to help trace the recent movements of coronavirus patients in order to establish virus transmission chains, attempting to slow the spread of the virus at all costs. This technological response to a global health crisis has brought questions around data privacy and security to the forefront. It forces state agencies, private companies, and individuals to wrestle with an essential question: How do organizations balance collecting data to solve problems for the public good while respecting individuals right to privacy in the 21st century? This question is increasingly relevant for TxDOT as an agency that collects and stores sensitive data related to travel patterns, personal information of residents who participate in programs and public engagement, toll payment information and other pieces of sensitive data. This paper explores key strategies that public agencies, regulators, and private companies can take to keep consumer data safe and decrease the risk of a malicious data breach.

Data Privacy, Security, and Consumer Protection

White Paper



KEY STRATEGIES

01

Create strong privacy principles

The first step for a responsible approach to data safety is to develop core data privacy principles. These shared, fundamental values will provide direction to the organization's employees, the public, and the private mobility companies who handle sensitive data.

02

Develop diverse, interdepartmental teams to implement privacy principles

In order to operationalize the privacy principles, a culture of privacy must be built and maintained throughout the organization. This requires training and buy-in from staff and third-party partners.

03

Follow federal policy updates and other states' policies

Take direction from other states and federal policies to guide implementation of an internal privacy and security plan to ensure alignment.

04

Allocate appropriate resources for enforcement of data privacy and security

Good privacy principles and transparent policy are the foundation for any meaningful privacy and security program, however, without proper resources for enforcement, outreach, and education the policies will not be sufficiently implemented.

05

Work in collaboration with private sector partners

When implementing privacy principles and security practices it is necessary to balance enforcement with encouragement. Maintain clear, open communication and provide resources and support to aid private partners in following regulations, practices, and policies.

Data Privacy, Security, and Consumer Protection

White Paper

INTRODUCTION

With the proliferation of various new technologies, which collect user data and track locations, users benefit from tailored services the ability to hail a car with their phone and navigate seamlessly from their current location to their next destination with ease. Similarly, companies can keep track of their devices like shared e-scooters and shared bikes as they are deployed on city streets, helping to keep their operations efficient. However, there are also some risks to consumers associated with having their mobility data collected, stored, and, in some cases, shared. Even when data is aggregated, sophisticated methods can often be used to match a user's identity with their location. These risks have sparked a robust conversation around data privacy, security, and consumer protections in relation to new transportation technologies.

In 2014 the New York Taxi and Limousine Commission (TLC) released taxi location data (over 173 million individual trips) for researchers to analyze. The identity of the taxi and driver for each trip had been protected by a data manipulation technique called "hashing". Hashing is a one-way encryption technique which replaces each drivers license number and taxi medallion number with an alphanumeric code that can't be reverse engineered to determine the original information. However, a computer programmer was able to determine where and when celebrities got in and out of New York taxis using publicly available sources like celebrity gossip blogs and when he combined this information with the TLC data, he was able to pinpoint actor, Bradley Cooper's exact destinations and route and how much he paid for the cab[1]. There have been other instances of industrious programmers using a combination of aggregated geolocation data and other publicly available data or media to reverse engineer the routes and locations of private citizens. Overall, Americans are concerned about their data being collected by companies and by governments. According to Pew Research Center, 81% of U.S. adults think the potential risks of companies collecting data about them outweigh the benefits--that's four out of five Americans.[2] This paper will catalogue various types of geolocation data and investigate the privacy risks and proposed legislation that may protect consumers on the federal, state, and local levels.

TRANSPORTATION DATA

There are many types of geolocation-related data that companies and governments collect and have access to including data generated from micromobility trips, public transit trips, ride-sharing trips, personal vehicles trips, automated and connected vehicle trips, and data collected via mobile phones through map and location applications. This section describes the specific types of data that is collected through each of these sources.

Micromobility

Shared micromobility refers to shared-use fleets of small, fully or partially human-powered vehicles such as bikes, e-bikes and e-scooters. Typically, these vehicles are rented through a mobile app or kiosk, are picked up and dropped off in the public right-of-way, and are meant for short point-to-point trips. Many cities across the United States have adopted the Mobility Data Specification (MDS), an Application Programming Interface (API) used to transmit anonymized information about micromobility vehicles and trips from a company such as Lime, Bird, or Jump to a city's active transportation or information technology department. This data specification requires the following pieces of data to be reported by the operator to the city: unique provider identification, provider name, device identification, vehicle identification number, vehicle type (bicycle, car, or scooter), propulsion type (human, electric assist, electric, or combustion), unique trip identification, time of trip, trip distance, routes, approximate level of route accuracy, trip start time, and trip end time. Other optional data includes:

publication time, parking verification (evidence of proper parking), standard cost of the trip, actual cost of the trip, and type of currency.[3]

Micromobility companies, however, are collecting far more data than what MDS is required to share with the cities who have adopted this data specification. If a micromobility user uses the login-through-Facebook function, many micromobility companies gain access to users' social media accounts including photos and other profile information. Companies such as Lime and Bird store this user information for an undefined amount of time and even after a user deletes his or her account. While the companies claim they do not sell data to third parties, they reserve the right to share user information with sponsors, business partners, and possibly advertisers.[4]

Third party data analysis companies have emerged as a buffer between the private mobility companies and the city governments who want access to trip data. Such intermediaries such as Populus, RideReport, and Inrix take in aggregated data and generate reports, visualizations, and analysis for city planning staff. Many in this industry feel that their city clients do not have a deep understanding of the privacy concerns that accompany the collection and storage of mobility data. For example, depending on the stringency of state laws accompanying the Freedom of Information Act, a city government could be forced to disclose the geolocation data it collects, putting citizens at risk.

Ride-Share

In the beginning of the ride-hailing technology boom, transportation network companies collected thousands of bits of data on their riders and drivers and suffered data breaches, which compromised their users' personal information.[5] Major ride hailing companies have since improved their privacy protocols and cybersecurity policies. However, new debates about who has access to this data persist. For example, Uber is facing several legal challenges from their drivers who want access to more detailed data related to their "dead time" GPS location, and customer service interactions. Some drivers and advocates feel that these data points demonstrate that drivers are "controlled by the platform." Thus, furthering the idea that drivers should be categorized as employers by law, not contractors.6 This question is being tested in California with the passage of California Assembly Bill 5, a state statute that entitles workers classified as employees to greater labor protections which do not apply to independent contractors. Concerns over employee misclassification in the "gig economy" drove support for the bill.

Some mobility companies refuse to submit real-time data to cities who demand it, claiming that it exposes their customers' sensitive location information. On the other hand, cities insist this data is needed to enforce fleet deployment regulations and other safety measures to manage the right-of-way. Many consumer protection groups have also warned cities about the risks of collecting sensitive geolocation information including the ACLU and the Electronic Frontier Foundation.

Vehicles

Personal vehicles have become data hubs with the introduction of more sensors and technology integrations. Many consumers are unaware that their cars are collecting data including their geolocation data and data which measures their driving tendencies and habits. More consumer protection measures are needed to ensure these companies minimize the data they collect, store it safely, and are transparent about how they use it, the entities with whom it shares, and the entities to whom it sells.

Connected vehicles are also producing data at prolific volumes. The Basic Safety Message (BSM) is a broadcast message typically transmitted up to ten times per second. BSM includes data such as vehicle size, position, speed, heading, acceleration, and brake system status. This data may be owned or discoverable by public agencies; and while it is incredibly valuable for enabling safety and mobility connected vehicle applications, it also contains

sensitive information that can reveal information regarding personal driving habits and travel behaviors. As more vehicles become equipped with connected vehicle technology, public agencies will need to develop the appropriate privacy and security management practices.

Public Transportation

Public transportation systems produce ridership data. This data is typically safe to analyze because there is no trip or route data assigned to a unique individual. However, in some cases where fare values can be attributed to specific riders or riders use their cell phones and credit card information to purchase transit fare, their geolocation data can become vulnerable to deanonymization attempts. One such case occurred in Australian in 2018. Public Transport Victoria released three years of travel records of Myki users. Myki is a fob-like transit pass which riders use to travel on trains, trams and buses in Melbourne and other parts of regional Victoria. Data scientists discovered that they could check their own Myki history online and match up their travel times with the data the transport agency released to ultimately reveal the entire three-year travel history of their card.[7]

Prospects of New Data from Connected and Automated Vehicles

Public agencies should structure partnerships to collect only data necessary for specific use cases and have a plan for data protection. In the future, automated and connected vehicles will generate reams of data. Currently it is unclear who will have access to this data and how it will be used. Since it is likely that automated vehicles designed for human transport will be deployed by a company and not driven or owned by individuals, a major question facing the introduction of this technology is: what party is responsible when there is an accident or malfunction? The insurance industry will need to create new products and procedures to ensure there is a clear process when an accident occurs— how will the costs (fiscal costs and liability) be distributed among stakeholders? Data from autonomous and connected vehicle behavior will be key in order to solve the questions posed above.[8]

POLICY UPDATE

Governing bodies from the European Union to the California State Legislature have been active in proposing and adopting new regulations and creating new agencies to protect their citizens' personal information. The following sections summarize these efforts and highlights some key lessons for legislators and privacy advocates.

General Data Protection Regulation

The General Data Protection Regulation (GDPR) was adopted by the European Union on May 26, 2018 in order to ensure that the processing of personal data must be lawful, fair and transparent, carried out with a strict purpose limitation, based on the principle of data minimization, and always with appropriate security.[9] The Information Commissioner's Office (ICO), led by Elizabeth Denham, is responsible for creating and upholding these new data regulations. The ICO focuses on protecting consumers from companies which may collect, share, and/ or sell personal information data in unethical or nontransparent ways. Key attributes of the GDPR:

- The most critical part of the legislation, and the part that created the political will for change was the age appropriate design code. A code that focuses on privacy by design and privacy by incorporating data privacy into products that kids use such as some smartphone applications.
- Regulators should be curious and innovative. The balance between enforcing change and encouraging change is important. Regulators need to understand the impact of privacy regulations on fair competition and markets.

The regulating authority should have a constructive dialogue with companies and offer support and tools that explain the regulations and give them what they need to get data security right. Most of the ICO's budget goes to proactive assistance.

- A good law is important, but the enforcement actions and advisory functions, willingness of regulators to listen are equally if not more important.
- The world will not be the same five years from now, so legislation should be "principle based" not didactic.

Federal

Consumer Online Privacy Rights Act

- Introduced in November, 2019 by U.S. Senator Cantwell, the Consumer Online Privacy Rights Act (COPRA) is a bill that provides a comprehensive consumer data privacy legislative framework. Key attributes of COPRA include:10
- Individuals who suffer from violation of the act may seek damages, equitable and declaratory relief and attorney's fees via a civil suit.
- COPRA designates a new bureau of the Federal Trade Commission as responsible for enforcement of the act in addition to State Attorneys General and consumer protection officers.
- It will not preempt state law, if state law affords the consumer greater protection.
- COPRA allows covered businesses to charge privacy-minded consumers a higher-price or provide a lower quality.
- "Precise geolocation" is considered sensitive data by COPRA.
- Under COPRA businesses must minimize data processing, not transfer data in a deceptive or harmful way, conduct an impact assessment for any algorithmic decision making, build a privacy protection system, and publish a privacy policy.

Consumer Data Privacy Act of 2019

After COPRA was introduced by Democratic Senator Maria Cantwell, Commerce Committee Chair Roger Wicker released a "staff discussion draft" of a consumer data privacy act of 2019. The two bills have many similarities and some differences. Those differences include:

- The Wicker bill does not provide details about how companies will assess data privacy outcomes, while COPRA does.
- The Wicker bill allows the FTC to send cases of possible discrimination to federal and state agencies while COPRA explicitly prohibits processing personal data in discriminatory ways.
- The Wicker bill will preempt any state law related to data privacy, while COPRA will only preempt in some cases.
- The Wicker bill does not allow for private rights of action.

Overall, COPRA is more detailed in its assessment requirements and implementation whereas the Wicker bill allows wider latitude for existing business and data practices. Both proposals raise individual privacy protection beyond existing federal law and the California Consumer Privacy Act. However, both bills also only apply to private companies, excluding government-run entities from the data requirements. [11]

Data Privacy, Security, and Consumer Protection

White Paper

States

States from Maine, to Texas, and California have proposed data privacy legislation to address consumer protection and data privacy in their jurisdictions. So far, California, Maine, and Nevada are the only states to pass data privacy acts. The California Consumer Privacy Act (CCPA) became effective on January 1, 2020.

California

The CCPA was designed to protect five rights of California consumers including: (1) The right of Californians to know what personal information is being collected about them; (2) The right of Californians to know whether their personal information is sold or disclosed and to whom; (3) The right of Californians to say no to the sale of personal information; (4) The right of Californians to access their personal information; (5) The right of Californians to equal service and price, even if they exercise their privacy rights.

States from Maine, to Texas, and California have proposed data privacy legislation to address consumer protection and data privacy in their jurisdictions.

Many privacy advocates like the ACLU and the Electronic Frontier Foundation believe the CCPA does not go far enough because it only covers the most sensitive personal information such as Social Security numbers, credit cards, or health information. Furthermore, the CCPA is unclear concerning the what enforcement will look like. It only states that the attorney general's office will be responsible for enforcement.[12] Other critics such as Uber believe that the law should extend its reach to cover government agencies which collect and store citizens' personal data.

Maine

Maine's "An Act to Protect the Privacy of Online Customer Information" will go into effect on July 1, 2020. This legislation is solely focused on the customer data collected by Internet Service Providers (ISPs). It necessitates that ISPs solicit consent from their customers to share or sell their data.

Texas

There have been two recent attempts to pass privacy legislation in the Texas legislature including the Texas Consumer Privacy Act (TXCPA) and the Texas Privacy Protection Act (HB 4390). The TXCPA is similar to the CCPA in that it would allow consumers to know what information is being collected about them, opt-out of sales of their information, and provide a process for their information to be deleted. The TXCPA, however, does not require businesses to implement and maintain data security procedures. TXCPA would be enforced by the Texas attorney general. It is unclear what additional resources, if any, would be made available to enforce TXCPA.

HB 4390 imposes similar rules as the TXCPA, but would only apply to businesses that have more than 50 employees or collected personally identifiable information of more than 5,000 individuals and have a gross revenue of more than $25 million or get 50% or more of its annual revenue from processing personally identifiable information. Neither the Texas Consumer Privacy Act nor the Texas Privacy Protection Act contain private cause of action for a security breach of personally identifiable information. Both pieces of legislation permit the Texas Attorney General to bring an action and recover civil penalties.

Ultimately these attempts to provide more protections for consumers are stop gap measures. States will continue to pursue a patchwork of various regulations until the federal government provides direction or enforces a national privacy and data security standard.

Local

In addition to privacy legislation on the state-wide level, many municipalities have taken on the challenge of data privacy themselves.

Data Privacy, Security, and Consumer Protection

White Paper

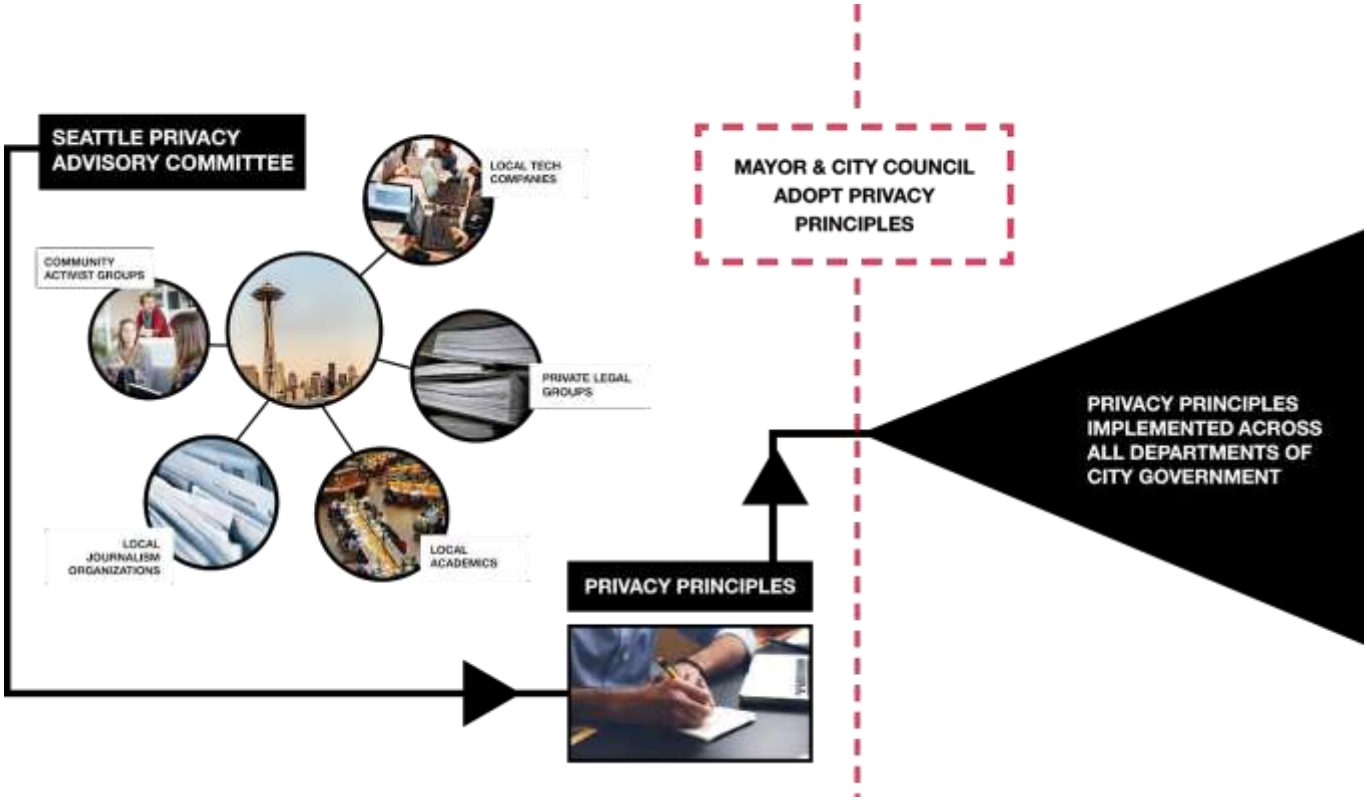


Figure 1: City of Seattle Privacy Advisory Committee

Seattle

Seattle is a leader in data privacy on the municipal level. In 2014, the community advocates and city council recognized the need to make privacy a key value as the city invested in new "Smart City" technologies and began to collect data to quantify how citizens were using public space and public infrastructure. The city council and mayor came together to address data privacy risks and build trust with their constituents by hiring a Chief Privacy Officer and create a Privacy Advisory Committee.

The committee, made up of stakeholders from business, journalism, activist groups, cyber security firms, and Washington University faculty, collaborated with city staff to craft a set of privacy principles.

The principles include:

1. We value yourprivacy
2. We collect and keep only what we need
3. How we use your information
4. We are accountable
5. How we share your information
6. Accuracy is important

Once the principles were created, the city council and mayor adopted them in a city ordinance and designated resources to operationalize them across 38 departments of Seattle's city government. The privacy team performs risk analysis, consultation, and work with all city departments to mitigate privacy risk. The office of privacy has been integrated into all purchasing, project management, and program development activities. The keys to Seattle's success in implementing and operationalizing these privacy principles has been

interdisciplinary team building, allocating significant resources towards this effort, and creating a culture of data privacy and security with ambassadors who work in each department. They create accountability and transparency by informing citizens what data they collect and issuing quarterly reports which communicate their progress towards living out the privacy principles.

Oakland Privacy Advisory Commission.

In 2016 the Oakland City Council narrowly agreed to create the Oakland Privacy Advisory Commission, a committee of council-appointed community members who review local government programs and policies through a data privacy lens. The creation of the commission was the result of years of activist activity in which residents protested the implementation of some data collection practices, which city agencies were deploying. For example, in 2013 the city received Department of Homeland Security funding for a Domain Awareness Center (DAC), which collected surveillance data from across the city. It started as a security project for the airport and port but ballooned to include information from over 700 cameras, gun detectors, and license plate readers. Community members organized against these surveillance measures and demanded to be educated about what data was being collected in and about their community. Oakland is the only city in the country to have such a council.

PRIVACY & SECURITY

Government DataBreaches

In 2019 alone, 966 government agencies, educational institutions, and healthcare providers in the United States faced ransomware attacks in which nefarious third parties attempted to steal individuals' confidential data and hold it ransom until the targeted institution pay a ransom fee. These data breaches, however, did more than inconvenience the institutions who were victimized by the attacks. They caused serious risk to citizens health and safety. In some cases, medical records were inaccessible or lost, 911 services interrupted, and police were locked out of background check systems.[13] These incidents were especially prevalent in 2019 because many government agencies lack appropriate cybersecurity standards for the modern age. A report issued by the state auditor of Mississippi after a cyberattack identified weaknesses in the state's defenses such as not having a security policy plan or disaster recovery plan in place, not performing legally mandated risk assessments, and failing to encrypt sensitive information.[14]

In 2017 Texas State Representative Capriglione filed House Bill 8 and House Bill 9, known as the Texas Cybersecurity Act and Texas Cybercrime Act. These acts provide specific measures to protect sensitive data and maintain readiness in the event of a cyber- attack. With these bills, the legislature designated $30.6 million for system upgrades at various state agencies with the Department of Information Resources (DIR) playing a key role in implementation. The DIR has established a biennial information security assessment and report mandatory for all state agencies. This is a step in the right direction for Texas agencies, however, cybersecurity best practices suggest that security assessments and audits conducted by an outside, third party term are more effective. These acts provide statewide agencies with some good tools to protect themselves from potential cyberattacks, however more focus needs to be placed on county and city-wide agencies, which also store and handle sensitive information. For example, in 2016 Tarrant County's 911 system was hacked by a college student who created a link, which he posted to Twitter. When a user clicked this link, their phone would automatically dial 911. The dispatch officers reported at least 850 hang-up calls during the attack, leading to drastically increased response times.[15]

Privacy principles create accountability and transparency by informing citizens about what data is being collected.

Data Privacy, Security, and Consumer Protection

White Paper

OPPORTUNITIES FOR TEXAS

The Texas Department of Information Resources (DIR) provides Agency Security Plan resources to educate agencies around the state about data security and to help them keep their data safe. The plan's template was created in collaboration with the private sector and includes five functions: Identify, protect, detect, respond, and recover. Within these five areas, DIR identifies 46 distinct security objectives and provides some strategies to meet the objectives. This framework is useful; however, it is not grounded with a foundation of explicit, transparent privacy principles—often the first step in creating a framework for how to approach data security and privacy. Moving forward, Texas has the opportunity to better communicate its approach to data protection and privacy by establishing clear, plain privacy principles and creating an interagency plan for implementing and operationalizing these principles while encouraging a culture of privacy and data collection minimization.

Considerations for Texas Public Agencies

- Regulation and internal privacy policies should be principle based. Start with strong privacy principles, then create diverse internal teams to "operationalize" the principles. Key examples are GDPR and Seattle Privacy Advisory Committee.
- A good law or regulation is important, but it is only the tip of the iceberg. Providing the necessary resources for enforcement in terms of labor and program funding is key.
- While Federal legislation would streamline and strengthen the protection and enforcement process for data privacy, local governments should retain some deference to manage privacy in their communities and on their streets.
- Regulating authority should have a constructive dialogue with companies and offer support and tools that explain the regulations and give them what they need to get data security right.

BIBLIOGRAPHY

[1]Johnston, A. (2015, April 19). Bradley Cooper's Taxi Ride: A Lesson in Privacy Risk. https://www.salingerprivacy.com.au/2015/04/19/bradley-coopers-taxi-ride-a-lesson-in-privacy-risk/

[2]Pew Research Center. (2019, November). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

[3]Open Mobility Foundation. (2019, February). Mobility Data Specification: Provider. https://github.com/openmobilityfoundation/mobility-data-specification/blob/dev/provider/README.md#trips

[4]Conway, N. (2018, July 25). Electric Scooters Are Racing to Collect Your Data. https://www.aclunc.org/blog/electric-scooters-are-racing-collect-your-data

[5]Lohrmann, D. (2017, December 2). After Uber Data Breach: Lessons for All of Us. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/after-uber-data-breach-lessons-for-all-of-us.html

[6]Holder, S. (2019, August 22). For Ride-Hailing Drivers, Data is Power. https://www.citylab.com/transportation/2019/08/uber-drivers-lawsuit-personal-data-ride-hailing-gig-economy/594232/

[7]Taylor, J. (2019, August 15). Myki data release breached privacy laws and revealed travel histories, including of Victorian MP. https://www.theguardian.com/australia-news/2019/aug/15/myki-data-release-breached-privacy-laws-and-revealed-travel-histories-including-of-victorian-mp

[8]Anderson, J., Kalra, N., Stanley, K., and Morikawa, J. (2018). Rethinking Insurance and Liability in the Transformative Age of Autonomous Vehicles. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF383/RAND_CF383.pdf

[9]General Data Protection Regulation. (2018). *Official Journal* L 119, 04.05.2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[10]Schwartz, A. (2019, December 3). Senator Cantwell Leads With New Consumer Data Privacy Bill. https://www.eff.org/deeplinks/2019/12/sen-cantwell-leads-new-consumer-data-privacy-bill

[11]Kerry, C. (2019, December 3). Game On: What to make of Senate Privacy Bills and Hearing. https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/

[12]Morrison, S. (2019, December 30). California's New Privacy Law, Explained. https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained

[13]Emsisoft Malware Lab. (2019, December 12). The State of Ransomware in the US: Report and Statistics. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

[14]White, S. (2019, October 1). Mississippi Government Offices Potentially Putting Taxpayer Data and Privacy. https://www2.osa.ms.gov/news/auditors-report-shows-disregard-for-cyber-security-in-state-government/

[15]Benton, J. (2019, March). Cyberdefense for Texas State Government. https://comptroller.texas.gov/economy/fiscal-notes/2019/mar/tx-cyberdefense.php