CONGESTION PRIVACY

The Surprising Privacy Toll of New York City's Proposed Congestion Pricing System

JANUARY 15, 2020

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

ENGELBERG CENTER
on Innovation Law & Policy
NYU School of Law

INTRODUCTION

There is no dispute that traffic is on the rise in major United States cities and around the world. New York City is no exception—it is estimated that New Yorkers spent an average of 133 hours sitting in traffic last year and, in many areas, it is faster to walk than it is to drive.[1] At the same time, the City's aging subway system suffers from deteriorating infrastructure, which has resulted in overcrowding and more frequent delays. In 2019, the State of New York enacted the MTA Reform and Traffic Mobility Act, which seeks to solve both of these problems by implementing a cordon-based congestion pricing program, whereby drivers will be charged a variable toll to enter and drive within certain areas of Manhattan. Alarmingly, however, congestion pricing may cost New Yorkers more than the planned tolls—the program could compromise their core privacy rights.

Without proper protections, congestion pricing will provide the City with a database on the day-to-day movements of individuals. By its nature, congestion pricing requires the collection of certain personal information from drivers who enter the tolling zone, including the time and date that the vehicle entered the zone. The choice of data-collection technologies, as well as the manner in which the program uses and discloses this information, may have far-reaching effects on driver privacy. For example, tolling programs frequently use automated license plate recognition[2] ("ALPR") technology for collection and enforcement purposes. ALPR technology often records information—such as images of a vehicle's occupants and surroundings—well beyond that necessary for toll collection. Absent appropriate safeguards, this information could be used for general law enforcement or other purposes wholly unrelated to congestion pricing and inconsistent with drivers' reasonable privacy expectations.

In this white paper, we consider the means by which congestion pricing can be implemented to reduce traffic without materially compromising individuals' right to privacy. In particular, this white paper focuses on the various technologies that might be deployed to implement congestion pricing, and the implications of these technologies on individual privacy. We explain why the current legal framework may not protect New Yorkers' privacy interests in data collected by the tolling infrastructure and provide recommendations for reducing encroachment on individual privacy while simultaneously advancing the goal of resolving New York City's transit problems.

[1] INRIX: Congestion Costs Each American 97 hours, $1,348 A Year, Press Release, *available at* http://inrix.com/press-releases/scorecard-2018-us/.

[2] Devices equipped with this technology are also referred to as automated license plate readers.

Part 1: Background

What is Congestion Pricing?

Congestion pricing aims to reduce traffic congestion in specified areas by charging drivers to use the roads in those areas during certain timeframes. By charging a toll to use roads, vehicles that do not have to use a particular road at a particular time are incentivized to use alternative means of transportation, such as public buses or trains, or to travel during off-peak times.[3] According to the Federal Highway Administration, a reduction of even 5% of the number of vehicles on a highly traveled road can have a meaningful impact on the flow of traffic.[4] Congestion pricing has been characterized by economists as "the single most viable and sustainable approach to reducing traffic congestion."[5]

Congestion pricing programs typically fall into one of four categories:

- *Variable Lane Pricing*. Drivers pay a toll to use certain dedicated lanes (e.g., express or high occupancy toll lanes). Fees may be fixed or variable based upon occupancy, time of day, or other factors.
- *Variable Roadway Pricing*. An entire roadway is usable only upon payment of a toll, which varies depending upon conditions.
- *Zone-Based Pricing*. Drivers pay a toll to drive within specified areas of a city. Zones where charges apply typically are heavily congested urban areas. The primary means of assessing zone-based fees are cordon charges, whereby vehicles are charged a fixed or variable fee for crossing a specified boundary, and area charges, whereby vehicles are assessed a toll for moving within a zone, whether or not the trip originated outside or inside of the zone.
- *Area-Wide Pricing*. Per-mile tolls are assessed on a variable basis within a specified area depending upon level of congestion, type of vehicle, time of day, or other factors.[6]

Revenues generated from congestion pricing may be used for a variety of purposes, such as improving highway and public transit infrastructure. As public transit options become more reliable due to infrastructure upgrades funded by congestion pricing, traffic may be further reduced.

[3] U.S. DEP'T. OF TRANSP., FED. HIGH. ADMIN., Congestion Pricing: A Primer at 1, Dec. 2006, *available at* https://ops.fhwa.dot.gov/publications/congestionpricing/congestionpricing.pdf.

[4] *Id.*

[5] *Id.*

[6] U.S. DEP'T. OF TRANSP., FED. HIGH. ADMIN., Technologies That Enable Congestion Pricing: A Primer, Oct. 2008, *available at* https://ops.fhwa.dot.gov/publications/fhwahop08042/fhwahop08042.pdf ("FHA Technology Primer").

Where and How Has Congestion Pricing Been Implemented?

To date, a number of cities around the world have implemented congestion pricing programs. Of relevance here, zone-based programs have been established in cities such as London, Stockholm, Singapore, and Milan. Although New York City is the first city in the United States to adopt legislation requiring implementation of a cordon-based tolling program, similar systems are being evaluated in other major U.S. cities, including San Francisco, Los Angeles, and Seattle.[7]

London. In 2003, the city of London implemented a zone-based program using area pricing. Under this program, vehicles pay a fee for entering and driving within a specified zone.[8] Currently, there is a weekday fee of £11.50 (approximately $12.50) for driving within the "charging zone" in and around the City of London.[9] The daily fee can be paid in advance or on the day of travel, or it can be paid the next charging day (in which case the fee increases to £14, or approximately $15).[10] Payment of the daily fee permits vehicles to enter, drive within, leave, and reenter the charging zone as often as desired in a single day.[11] City-licensed taxis and buses, wheelchair-accessible private hire vehicles, motorcycles, and bicycles are exempt from payment of the congestion charge.[12]

In London, the charging zone is marked by signage; there are no toll booths or other barriers to entry.[13] The congestion-based charge is assessed through a network of 197 camera sites that monitor "every single lane of traffic at both exit and entry points to the charging zone."[14] The cameras are equipped with ALPR technology, which records images of vehicles that enter, leave, or drive within the charging zone.[15] The images are used to create a record demonstrating that a particular vehicle was in the charging zone at a designated time.[16] The information captured by the ALPR-enabled cameras includes an alphanumeric image of a

[7] *See*, *e.g.*, Laura J. Nelson, *Pay $4 to Drive to the Westside? Congestion Pricing Could Cut Traffic Gridlock, Report Says*, L.A. Times, Mar. 28, 2019, https://www.latimes.com/local/lanow/la-me-ln-congestion-pricing-toll-traffic-westside-20190328-story.html.

[8] Transp. for London, Congestion Charge/ULEZ Zone, https://tfl.gov.uk/modes/driving/congestion-charge/congestion-charge-zone. There is no charge to drive in the charging zone on weekends Bank Holidays, or the days between Christmas Day and New Year's Day. *Id.* Residents of the charging zone are eligible to receive a 90% discount. *Id.*

[9] *Id.*

[10] Transp. for London, Congestion Charge Payments, https://tfl.gov.uk/modes/driving/congestion-charge/paying-the-congestion-charge.

[11] Transp. for London, Congestion Charge Factsheet, http://content.tfl.gov.uk/congestion-charge-factsheet.pdf.pdf ("TfL Factsheet").

[12] *Id.*

[13] *Id.*

[14] Transp. for London, What do I need to know about the central London Congestion Charge camera system? (Jan. 2011), http://content.tfl.gov.uk/cc-cameras.pdf ("TfL Camera Facts").

[15] *See* TfL Factsheet, *supra* note 11.

[16] *See* TfL Camera Facts, *supra* note 14.

vehicle's license plate (referred to in London as a Vehicle Registration Mark ("VRM") as well as a photographic image of the vehicle.[17] Images collected through the ALPR technology are encrypted and transmitted to a data center using a dedicated secure broadband link.[18] According to Transport for London ("TfL"), the agency responsible for implementing the program, "images . . . show a vehicle, its registration number and the immediate surroundings."[19] The agency notes that in some cases the image includes the occupants of a vehicle or other individuals in the immediate area.[20]

Images collected by the ALPR-enabled cameras are matched against a database to determine whether the daily fee has been paid for the VRM, or if the VRM is exempt from payment.[21] If a VRM is matched in the database as having paid the fee (or as exempt from such payment), then the images of the vehicle are automatically erased by midnight of the next charging day (except that, for auto-pay vehicles, ALPR data and images are retained for up to two months to allow for the account to be settled).[22] If a vehicle is photographed within the charging zone and there is no record of timely payment (or exemption), then TfL contacts the Driver and Vehicle Licensing Agency to obtain information regarding the vehicle's registered owner (e.g., name and address) and sends the owner a penalty charge notice.[23] For vehicles subject to a penalty charge notice, information (including images of the subject vehicle) may be retained for as long as seven years after the charge has been settled.[24]

TfL uses and makes congestion pricing information available for a number of reasons, including disclosing data to law enforcement[25] and using data for purposes of implementing the

[17] Transp. for London, Road User Charging (July 2019), https://tfl.gov.uk/corporate/privacy-and-cookies/road-user-charging ("TfL Road User Charging Policy"). According to a 2011 publication by TfL, the cameras collect black and white photographs of a VRM, as well as color photographs that take "a wider 'contextual' image of the relevant vehicle." TfL Camera Facts, *supra* note 14.

[18] *See* TfL Camera Facts, *supra* note 14.

[19] Transp. for London, Subject Access Request (Apr. 2018), *available at* http://content.tfl.gov.uk/road-user-charging-subject-access-request-form.pdf ("TfL Road User Personal Data Request Form").

[20] *Id.*

[21] *See*, *e.g.*, TfL Factsheet, *supra* note 11.

[22] *See* TfL Camera Facts, *supra* note 14. *See also*, TfL Road User Charging Policy, *supra* note 17.

[23] Transp. for London, Newly Purchased Vehicles, https://tfl.gov.uk/modes/driving/congestion-charge/penalties-and-enforcement/newly-purchased-vehicles.

[24] TfL Road User Charging Policy, *supra* note 17.

[25] TfL may disclose data in response to a "valid" request by police. TfL Road User Charging Policy, *supra* note 17. It is not clear what constitutes a "valid" police request, as this determination is made by TfL on a case-by-case evaluation of whether police have demonstrated that the requested data relates to investigation of a specific crime and whether the disclosure would comply with applicable law. *Id.* TfL has an agreement with the Metropolitan Police Service ("MPS") to provide access to data collected by TfL in connection with matters related to "national security"—a potentially broad-reaching directive. *Id.* In addition, MPS has real-time access to the ALPR cameras used by TfL for London's congestion pricing program for general crime prevention purposes, though reportedly no images of vehicles are provided in this connection. *Id.*

program.[26] TfL promises that "personal information will be properly safeguarded and processed in accordance with privacy and data protection legislation,"[27] but the steps that it takes to fulfill this promise are not readily apparent in the privacy policies governing TfL's use of personal information collected in connection with congestion pricing, which includes disclosure to law enforcement and third party service providers. TfL has a process by which an individual driver may request access to all information about themself and any vehicles registered to the driver.[28]

Since congestion pricing was implemented in 2003, London has experienced a reduction in traffic, with approximately 80,000 fewer cars entering the charging zone than in 2002,[29] and average speeds increasing by 30%.[30] The program has resulted in improved public transit systems, cleaner air, and safer roads.[31]

Stockholm.[32] The city of Stockholm deployed a cordon-based program in 2007, after implementation of a seven-month pilot program. In Stockholm, vehicles that pass a control point on weekdays between the hours of 6:30 a.m. and 7:30 p.m. are charged a variable fee, subject to a maximum rate of SEK 105 (approximately $11), with the highest rates imposed at times and places when traffic is heaviest. Then-current rates are displayed on digital screens visible at control points. Emergency vehicles, buses over a specified weight, motorbikes, mopeds, and certain other vehicles are exempt from congestion pricing charges. Beginning in 2013, Stockholm's congestion pricing system was expanded to Gothenburg (the second largest city in Sweden).

As is the case in London, Stockholm's congestion pricing program relies on cameras. When a vehicle passes one of 18 control points around the city, cameras equipped with ALPR photograph the vehicle's license plate. Stockholm's system uses cameras only at the congestion-zone entry and exit points, and does not collect information as vehicles drive within the zone. The images collected at the control points are cropped to show only a vehicle's license plate and the cropped images are encrypted and sent, along with information regarding the location, time, and date the image was captured, to the Swedish Transport Authority ("STA")

[26] *See, e.g.,* TfL Road User Personal Data Request Form, *supra* note 19. In this connection, TfL has agreements with third-party service providers to whom it might make information, including images, available in connection with day-to-day operations. TfL Road User Charging Policy, *supra* note 17. TfL also shares information with other agencies, such as the Environment and Traffic Adjudicators, the Traffic Enforcement Centre, or other debt collection agencies, in order to collect and enforcement payments, as well as to "prevent and detect crime, trace and recover unpaid debt and protect public funds." TfL Road User Personal Data Request Form, *supra* note 19.

[27] *Id.*

[28] *See* TfL Road User Personal Data Request Form, *supra* note 19.

[29] TfL Factsheet, *supra* note 11.

[30] FIX NYC Advisory Panel Report, 12 (Jan. 19, 2018), *available at* www.hntb.com/HNTB/media/HNTBMediaLibrary/Home/Fix-NYC-Panel-Report.pdf.

[31] TfL Factsheet, *supra* note 11.

[32] Information regarding Stockholm's congestion pricing system is based upon an interview with Jonas Eliasson, Professor of Transport Systems, Linköping University, as well as materials posted to the Transport Styrelsen website at https://www.transportstyrelsen.se/en/road/Congestion-taxes-in-Stockholm-and-Goteborg/.

for vehicle identification.[33] At the end of each month, the STA sends a monthly invoice to owners of vehicles registered in Sweden.[34] The data collected through Stockholm's congestion pricing system is retained until approximately three to four months after the applicable fee is paid, at which time the data is deleted (though data may be retained longer in the event of a fee dispute or complaint).

Vehicle-specific data retained in Stockholm's system may not be routinely accessed. For example, images and information collected about a particular vehicle are not typically reviewed unless there is a dispute or complaint regarding a fee. Nor is such information generally accessible by third parties, including the police. Although it is technically possible that data collected through Stockholm's congestion pricing program could be used to track driver movements, there are strict laws in Sweden that limit the type of data that can be retrieved from the system and the circumstances under which such data can be accessed. That said, aggregate, non-individualized data (e.g., the total number of vehicles entering the congestion zone from a given municipality) obtained through Stockholm's ALPR-enabled cameras has been used for traffic forecasting and analysis.

Singapore.[35] Singapore has used a cordon pricing to manage traffic since 1975. In 1998, Singapore began using Electronic Road Pricing ("ERP"), whereby vehicles that pass an ERP gantry between the hours of 7 a.m. and 8 p.m. Monday through Saturday (except holidays) are charged a variable fee ranging from S$0–S$3 (approximately $0–$2) depending upon the location of the vehicle, the time of day, and the amount of traffic. The fee is assessed through in-vehicle transponders and roadside gantries installed at over 80 locations within and surrounding the central business district.[36] Under this system, ERP gantries use radio spectrum to communicate with a vehicle's transponder each time the vehicle passes through a gantry. The then-applicable charge is deducted automatically from a stored value card or credit card inserted into the transponder. The ERP gantries use cameras equipped with ALPR to monitor vehicles.[37]

[33] Jonas Eliasson, KTH Royal Institute of Technology, *The Stockholm Congestion Charges: An Overview,* CENTRE FOR TRANSP. STUDIES STOCKHOLM, 2014, *available at* http://www.transportportal.se/swopec/cts2014-7.pdf.

[34] The STA has contracted with a third party, EPass24, to conduct monthly invoicing and payment collections for vehicles registered in countries other than Sweden. *See* SWEDISH TRANSP. AGENCY, EPASS24: The Swedish Road Toll System, https://www.epass24.com/.

[35] Information regarding Singapore's congestion pricing program is based upon materials posted to the website of the Land Transport Authority of Singapore at, *e.g.*, https://www.lta.gov.sg/content/ltaweb/en/roads-and-motoring/managing-traffic-and-congestion.html and https://va.ecitizen.gov.sg/cfp/CustomerPages/LTA/explore_faq.aspx.

[36] TRI-STATE TRANSP. CAMP., Road Pricing in London, Stockholm, and Singapore: A Way Forward for New York City, 15 (2018), *available at* http://www.tstc.org/wp-content/uploads/2018/03/TSTC_A_Way_Forward_CPreport_1.4.18_medium.pdf.

[37] Enrique Dans, *Congestion Charges Are A Welcome Sign Of The Times*, FORBES, Apr. 2, 2019, https://www.forbes.com/sites/enriquedans/2019/04/02/congestion-charges-are-a-welcome-sign-of-the-times/#4bf7b8337474.

Singapore is transitioning to a new satellite-based system to assess congestion-based fees on drivers. This system, which is expected to be operational in 2020, will use Global Navigation Satellite System spectrum, and will require drivers to replace their transponders with new on-board units capable of supporting additional services, such as providing real-time traffic information.[38]

Milan.[39] In 2012, the city of Milan implemented a zone-based pricing program throughout "Area C," an 8.2 square kilometer zone within the city. Presently, there is a weekday fee of up to €5 (approximately $5.50) for a vehicle to enter Area C.[40] The daily fee can be paid by purchasing a single-day or multiple-day entrance ticket. Payment of the daily fee permits vehicles to enter Area C at 36 access points as often as desired during the period in which the entrance ticket is valid.[41] Electric, hybrid, and biofuel vehicles, as well as scooters, are exempt from payment of the congestion charge, as are vehicles entering Area C to drive to the hospital under certain circumstances and those transporting disabled persons. Milan tracks vehicles entering an Area C access point with electronic gates and cameras equipped with ALPR technology to enforce Area C congestion pricing.[42]

What Does the New York Zone-Based Congestion Pricing Plan Propose to Do and How Will It Be Implemented?

In an effort to address increasing traffic and raise money to repair New York City's aging public transit system, New York State enacted the MTA Reform and Traffic Mobility Act (the "Traffic Mobility Act") in 2019.[43] Pursuant to the Traffic Mobility Act, the Triborough Bridge and Tunnel Authority ("TBTA") is authorized to implement a cordon-based congestion pricing program for the central business district of Manhattan ("CBD").[44] Funds raised by program are earmarked for capital improvements to the City's public transit system, as well as commuter rail

[38] *See, e.g.,* Eileen Yu, *Singapore to Implement Satellite Road Toll System from 2020*, ZDNET, Feb. 26, 2016, https://www.zdnet.com/article/singapore-to-implement-satellite-road-toll-system-from-2020/.

[39] Information regarding Milan's congestion pricing program is based upon materials posted to the Area C website at https://www.areacmilano.it/en.

[40] Congestion-based pricing is in effect from 7:30 a.m. to 7:30 p.m. Monday through Wednesday, as well as on Fridays, and from 7:30 a.m. to 6:30 p.m. on Thursdays. There is no charge to enter Area C on weekends or public holidays.

[41] There are 43 locations where vehicles can enter Area C, but seven of these locations are not available for use by the general public.

[42] C40 CITIES, *Milan's Area C Reduces Traffic Pollution and Transforms City Center*, Mar. 24, 2015, https://www.c40.org/case_studies/milan-s-area-c-reduces-traffic-pollution-and-transforms-the-city-center.

[43] 2019 N.Y. SB 1509, Part ZZZ (codified at NY CLS Veh & Tr, Title VIII, Art. 44-C). The Traffic Act is part of the as part of the 2019 state budget legislation, which was passed on March 29, 2019 and signed into law by Governor Cuomo on April 12.

[44] NY CLS Veh & Tr § 1704. The CBD consists of the area of Manhattan bounded by 60th Street at the north, Battery Park at the south, FDR Drive at the east and the West Side Highway at the west. *Id.*

systems serving New York City.[45] The earliest date on which drivers can be required to pay tolls in the CBD is December 31, 2020.[46]

The Traffic Mobility Act does not detail the specific manner in which congestion pricing must be implemented in New York City, nor does it contain any language aimed at ensuring that the program does not encroach upon individuals' privacy. Rather, the statute vests the TBTA with decision-making authority to design and develop a program to toll vehicles that "enter and remain in" the CBD.[47] Thus, for example, the TBTA has discretion to determine the technologies to be deployed in order to collect and enforce the payment of tolls, the nature and scope of the data to be amassed in connection with the program, and the terms and conditions under which such data will be used, disclosed, and retained. Although the TBTA is the agency tasked with implementing congestion pricing, the Traffic Mobility Act requires the TBTA to execute a Memorandum of Understanding ("MOU") with the City to coordinate and facilitate the deployment and operation of the congestion pricing system.[48]

[45] NY CLS Pub A § 553-j(2).

[46] NY CLS Veh & Tr § 1703(8).

[47] NY CLS Veh & Tr § 1703(2) and (4). The statute mandates that a six-member traffic mobility review board be established to recommend variable rate toll amounts to the TBTA, which will then make the final decision as to rates. NY CLS Pub A § 553-k. The traffic mobility review board is required to make its pricing recommendations to the TBTA board between November 15, 2020 and December 31, 2020. NY CLS Pub A § 553-k(2).

[48] NY CLS Veh & Tr § 1704(2-a).

Part 2: Privacy Risks

How Does A Congestion Pricing Traffic Management System Implicate Privacy?

As explained above, congestion pricing programs charge tolls for vehicles to use certain roads during specified time periods. Accordingly, in order to implement congestion pricing, it is necessary to obtain information regarding the time and date a vehicle is in a particular location. Location-based data, or geolocation data, is widely recognized as sensitive personal information. For example, the Federal Trade Commission ("FTC") considers location information to be personal information and has taken enforcement action against companies related to their use of location information.[49] Similarly, location information is among the type of personal information protected by federal law governing telecommunications records.[50] The United States Supreme Court has observed that location records provide "an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations."[51] International and state privacy laws also afford special protections to location information.[52]

The collection of location information is not the only way in which congestion pricing endangers privacy. The systems deployed to date rely on cameras equipped with ALPR both for toll collection purposes as well as for enforcement. However, images captured by these cameras often include more than just license plate data. ALPR-enabled cameras may capture images that show a vehicle's make and model, the driver and passengers, vehicle contents, or the vehicle's surroundings (including images of individuals or objects merely in the vicinity of a vehicle with which they have no connection). For example, ALPR-enabled cameras have been reported to have captured images of people getting in or out of their cars in their own driveways.[53]

Information collected by ALPR technology, including location information, can be readily linked to specific individuals, such as the registered owner of the car or individuals captured in license plate photographs.[54] Accordingly, data collected by a tolling program can reveal highly personal information about individuals, such as trips to doctors' offices, places of worship, or

[49] *See, e.g.*, In the Matter of Uber Technologies, Inc., Decision and Order, Docket No. C-4662 (defining personal information to include "precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information").

[50] *See* 47 U.S.C. § 222(h)(1)(A).

[51] *Carpenter v. United States*, 138 S.Ct. 2206, 2217 (2018) (citing *United States v. Jones*, 565 U.S. 400, 415 (2012) (opinion of Sotomayor, J.)) (internal quotation marks omitted).

[52] *See, e.g.,* EU General Data Protection Regulation (Regulation (EU) 2016/679), Article 4(1); CAL. CIV. CODE § 1798.140(o)(G).

[53] Gil Aegerter, *License Plate Data Not Just For Cops: Private Companies Are Tracking Your Car*, NBC NEWS July 19, 2013, https://www.nbcnews.com/news/world/license-plate-data-not-just-cops-private-companies-are-tracking-flna6C10684677.

[54] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller and Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, NY TIMES, Dec. 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

immigration-related locations.[55] The vast amount of data collected by ALPR-enabled cameras is frequently maintained in databases for extended periods of time,[56] such that ALPR data can be used to create a map of an individual's movements over days or even weeks, and also may be used to predict future behavior.[57] ALPR data is often readily shared with law enforcement and has led to the arrest of innocent people based on inaccurate database information.[58]

Will the City's Zone-Based Tolling Program Be Implemented In a Manner Likely to Encroach on Drivers' Privacy?

The TBTA's actions to date suggest the congestion pricing program will likely undermine New Yorkers' privacy. The TBTA has issued at least two requests for proposals regarding the technologies and systems that might be deployed in connection with congestion pricing.[59] The technologies under consideration include traditional, transponder-based radio frequency identification and camera-based ALPR technologies as well as new technologies, such as use of a vehicle's Bluetooth system or mobile applications. It is likely that any of these technologies will rely, at least in part, on ALPR technology to collect or enforce the payment of tolls.[60]

In requesting information regarding potential technologies, the TBTA has focused on how the technology will be installed and operated, and what data will be collected. To date, the TBTA has not publicly solicited feedback as to the privacy implications of any of the proposed technologies. That privacy is likely to be an issue is evidenced by the TBTA's statement that it is "seeking a solution that is highly scalable and capable of making swift transitions to more complex charging schemes such as those driven by congestion, distance traveled, and dwell time."[61] Implementation of these charging schemes would require tracking individual vehicles over time, as well as collecting data regarding a vehicle's movements within the CBD.

[55] *See*, *e.g.*, Tanvi Misra, *When Transit Agencies Spy on Riders*, CITYLAB, Sept. 18, 2018, https://www.citylab.com/equity/2018/09/when-your-transit-agency-is-found-tracking-you/570292/.

[56] For example, the Electronic Frontier Foundation reports that 173 agencies from 23 states and the federal government accounted for roughly 2.5 -billion license plate scans in 2016 and 2017. ELECTRONIC FRONTIER FOUNDATION, Automated License Plate Reader Dataset: What We Learned, https://www.eff.org/pages/what-we-learned.

[57] *See*, *e.g.*, ELECTRONIC FRONTIER FOUNDATION, Automated License Plate Reader Dataset: What Is ALPR?, https://www.eff.org/pages/what-alpr.

[58] *See, e.g.*, Lisa Fernandez, *Privacy Advocate Sues CoCo Sheriff's Deputies After License Plate Readers Target His Car Stolen,* KTVU, Feb. 15, 2019, http://www.ktvu.com/news/2-investigates/privacy-advocate-detained-at-gunpoint-when-licence-plate-readers-mistakenly-marked-his-car-stolen.

[59] Preliminary Solicitation No. 19-CBDT-2978, METROPOLITAN TRANSP. AUTH., STATE OF N.Y. (May 31, 2019), *available at* http://web.mta.info/bandt/procure/19-CBDT-2978%20LTR.pdf ("May RFP"); Request for Technology – 19-65 Congestion Pricing Alternative Technology, METROPOLITAN TRANSP. AUTH., STATE OF N.Y. (Mar. 28, 2019), *available at* http://web.mta.info/bandt/procure/RFI-19-65.pdf ("March RFP").

[60] *See* May RFP, *supra* note 59, at 1 (stating that the toll collection system "may use Radio Frequency Identification, Automatic License Plate Recognition, and/or other vehicle detection mechanisms" to "detect vehicles entering or remaining in the CBD."). *See also*, FHA Technology Primer *supra* note 5*.*

[61] May RFP, *supra* note 59, at 1.

The potential that technologies deployed for congestion pricing in New York City will intrude upon individuals' privacy is further evidenced by at least one proposal made in February 2019. At this time, Perceptics, a company that designs "vehicle identification and license plate recognition products,"[62] reportedly met with the Metropolitan Transit Authority ("MTA"), of which the TBTA is a part, to pitch its technology for use by the tolling program.[63] According to leaked documents, the Perceptics pitch proposed a system that would photograph a vehicle's license plate as well as the vehicle's occupants.[64] The Perceptics system would assign each vehicle a unique identifier and would utilize "'unique machine learning algorithms, allowing the city to immediately recognize and build travel histories of every car in the congestion zone."[65] Through the use of unique vehicle identifiers, vehicles could be tracked as they move throughout the City, even if a license plate image cannot be captured.[66] Regardless of whether the TBTA ultimately adopts the system proposed by Perceptics, the Perceptics proposal provides a concrete example of the scope of personal information that might be collected through the tolling program.

Similarly, the MOU between the TBTA and the City setting forth the division of responsibilities and general parameters for the implementation of congestion pricing raises questions regarding privacy.[67] The MOU contemplates that the TBTA and the City will share historical data regarding traffic at TBTA crossings, as well as prospective data relating to traffic entering the CBD. While the TBTA is required to anonymize certain data to exclude personally identifiable information, the MOU does not otherwise delineate the nature of the data to be shared between the parties, nor does it restrict the use or disclosure of such data. Accordingly, it is possible that the data sharing arrangement between the TBTA and the City might implicate New Yorkers' privacy, particularly if the shared data is provided to other third parties or used in combination with artificial intelligence ("AI") technologies.[68]

What Privacy Risks Do New Yorkers Face As a Result of Congestion Pricing?

The potential privacy risks associated with congestion pricing in New York depend in large part on the amount, and type, of data to be collected, as well as the extent to which such data is disclosed or used for other purposes. As described above, at its simplest, congestion

[62] PERCEPTICS, History & Team, https://www.perceptics.com/about/history-team/.

[63] *See* Sam Biddle, *Hacked Border Surveillance Firm Wants to Profile Drivers, Passengers, and Their "Likely Trip Purpose" in New York City*, THE INTERCEPT, July 9, 2019, https://theintercept.com/2019/07/09/surveillance-perceptics-new-york-city-drivers/.

[64] *Id*. (reporting that the technology pitched by Perceptics is apparently "capable of observing driver behavior, cell phone usage, and seat belt enforcement").

[65] *Id.*

[66] *Id.*

[67] *See* Memorandum of Understanding between TBTA and The City of New York Department of Transportation (June 11, 2019).

[68] *See* ELECTRONIC FRONTIER FOUNDATION, Automated License Plate Readers (ALPRs), https://www.eff.org/pages/automated-license-plate-readers-alpr (discussing how historical ALPR data has been used by law enforcement). *See also infra* at Part 2: What Privacy Risks Do New Yorkers Face As a Result of Congestion Pricing?

pricing will require the collection of the data necessary to determine when and where a vehicle has entered and traveled through the CBD, as well as to obtain payment from the driver. The collected data is likely to include location and other sensitive information. The privacy risks associated with the collection of this sensitive information stem from the potential for use and disclosure unrelated to congestion pricing, and thus not in accordance with driver expectations regarding the use of their personal information.

Disclosure to Law Enforcement

Unless protections are put in place, data collected for congestion pricing in New York City could be disclosed to and used by local, state, or federal law enforcement, including U.S. Immigration and Customs Enforcement ("ICE"), for purposes unrelated to those for which the information was collected. For example, as noted above, TfL, the agency implementing London's zoned-based tolling program, routinely provides the Metropolitan Police Service with access to London's ALPR-enabled cameras.

In the United States, local, state, and federal law enforcement agencies gain access to massive amounts of license plate data from vehicles across the country through databases maintained by private companies such as Vigilant Solutions ("Vigilant").[69] Through these databases, ALPR-collected data can be integrated with other systems to create individual-specific personal histories in a manner of seconds.[70] The New York Police Department ("NYPD"), for example, already has access to a swath of information collected by license plate readers through a contract with Vigilant and reportedly retains such data for at least five years.[71] Coupling this data with information collected through the City's tolling program would expand the NYPD's already massive surveillance databases, thereby enabling it (and potentially other law enforcement agencies) to track the movements of millions of innocent people.[72]

The NYPD is not the only law enforcement agency to rely on ALPR databases. For example, since 2016, Sacramento County welfare fraud investigators have used ALPR data supplied by Vigilant to locate suspects and collect evidence of fraud.[73] In addition to using ALPR

[69] Conor Friedersdorf, *An Unprecedented Threat to Privacy*, The Atlantic, Jan. 27, 2016, https://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/ (explaining that, in 2016, Vigilant Solutions had taken about 2.2 billion license plate photos, and that the company profits by selling this data to clients, including to about 3,000 law enforcement agencies).

[70] Brief of Amicus Curiae Electronic Frontier Foundation, Neal v. Fairfax Cty. Police Dep't, 16 (Feb. 22, 2017), https://www.eff.org/files/2017/02/22/neal_v._fairfax_pd_-_eff_amicus_brief_file_endorsed.pdf.

[71] Mariko Hirose, *Documents Uncover NYPD's Vast License Plate Reader Database*, ACLU, Jan. 25, 2016, https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database.

[72] *See id.*

[73] The Sacramento County Dep't of Human Assistance pays Vigilant about $5,000 per year to access the license plate data. Kellen Browning, *Sacramento welfare investigators track drivers to find fraud. Privacy group raises red flags*, The Sacramento Bee, Aug. 10, 2018, https://www.sacbee.com/news/local/article216093470.html. The County states that ALPR data is used only for "legitimate law enforcement purposes." Sacramento County Dep't

for their own purposes, law enforcement agencies also have shared ALPR data with other agencies, such as ICE, which reportedly has obtained ALPR data from over 80 local law enforcement agencies in over twelve states.[74] Notably, in at least one instance, ICE has obtained inadvertent access to ALPR data maintained by a transit authority.[75] Records of data collected via ALPR technology also have been used to track minority groups and monitor constitutionally protected activity.[76]

Artificial Intelligence

Disclosure of data collected for congestion pricing could be even more problematic if AI technologies are employed to search or "mine" the data. In New York, for example, the NYPD's AI systems already have the capability to "learn" a person's daily routine based upon data collected by ALPR technology.[77] The NYPD's AI tool uses algorithms to determine "possible associates" of criminal activity.[78] AI, however, has been shown to have a discriminatory impact.[79] AI bias and discrimination occurs when the data inputs do not represent reality (e.g., more pictures of lighter-skinned individuals are input into a facial recognition algorithm than pictures of dark-skinned individuals, such that the system has a higher error rate at recognizing darker-skinned individuals) or the inputs are based upon existing practices (e.g., an AI recruiting

of Human Assistance, ALPR Usage and Privacy Policy, https://ha.saccounty.net/Documents/License%20Plate%20Recognition%20Usage%20Policy.pdf.

[74] Vasudha Talla, *Documents Reveal ICE Using Driver Location Data From Local Police for Deportations*, ACLU, Mar. 13, 2019, https://www.aclu.org/blog/immigrants-rights/ice-and-border-patrol-abuses/documents-reveal-ice-using-driver-location-data.

[75] In 2017, cameras overlooking a parking lot in Oakland's MacArthur Station, the largest station in the Bay Area Rapid Transit (BART) system, used ALPR technology to capture over 57,000 license plate numbers. *See* Misra, *supra* note 55. In what the transit authority described as an accident, the license plate data was made available to ICE and other federal authorities. *Id.* The cameras were installed in 2015 as part of an effort to curb crime in the parking lot, but activation was put on hold due to concerns about the lack of a surveillance policy. *Id.* The transit agency stated that it confirmed that ICE did not use the data. *Id.*

[76] *See, e.g.*, Paul Lewis, *CCTV aimed at Muslim areas in Birmingham to be dismantled*, The Guardian, Oct. 25, 2010, https://www.theguardian.com/uk/2010/oct/25/birmingham-cctv-muslim-areas-surveillance; Adam Goldman and Matt Apuzzo, *NYPD Defends Tactics Over Mosque Spying; Records Reveal New Details on Muslim Surveillance,* Huffpost, Apr. 25, 2012, https://www.huffpost.com/entry/nypd-defends-tactics-over_n_1298997; Devlin Barrett, *Gun-Show Customers' License Plates Come Under Scrutiny*, Wall Street Journal, Oct. 2, 2016, https://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302.

[77] Ayyan Zubair, *Automated License Plate Readers & Law Enforcement*, Surveillance Technology Oversight Project, Inc., July 5, 2019, https://www.stopspying.org/latest-news/2019/7/5/automated-license-plate-readers-amp-law-enforcement.

[78] *Id.*

[79] *See, e.g.,* Joy Buolamwini, *Artificial Intelligence Has a Problem With Gender and Racial Bias. Here's How to Solve It.*, Time, Feb. 7, 2019, https://time.com/5520558/artificial-intelligence-racial-gender-bias/. Congress has held multiple hearings to collect information regarding the use of facial recognition technology and the privacy implications of facial recognition. In May and June, the U.S. House of Representatives Committee on Oversight and Reform held a two-part hearing on facial recognition technology. Additionally, in July 2019, the House Homeland Security Committee held a hearing to question Department of Homeland Security officials about their use of facial recognition technology.

tool dismissed female candidates based on historical hiring decisions).[80] Facial recognition technology, for example, is more likely to misidentify people of color (in particular, women of color),[81] as well as transgender, non-binary, and gender-nonconforming individuals.[82]

Nevertheless, AI is used by law enforcement to identify suspects and to determine where and how to concentrate their law enforcement efforts.[83] For example, the NYPD has used facial recognition software to identify celebrity "look-alike" suspects using celebrity photographs when crime scene photographs are too poor quality to return face recognition results.[84] Additionally, the NYPD has altered suspect images using photo editing software before running them through the face recognition database.[85] Law enforcement agencies that engage in practices such as these are conducting criminal investigations based on fundamentally unreliable or heavily edited evidence. Despite these flaws, use of facial recognition technology by law enforcement agencies, including ICE,[86] is widespread.[87] Accordingly, there is risk that data collected for congestion pricing could be mined for use in AI technologies, notwithstanding the known errors in both AI-produced results and ALPR collected data.[88]

[80] *See* Karen Hao, *This Is How AI Bias Really Happens—and Why It's So Hard to Fix*, MIT TECHNOLOGY REVIEW, Feb. 4, 2019, https://www.technologyreview.com/s/612876/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/.

[81] Steve Lohr, *Facial Recognition Is Accurate, If You're a White Guy*, NEW YORK TIMES, Feb. 9, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html?module=inline. A peer-reviewed study published in January 2019 showed that Amazon's facial recognition technology, Rekognition, mistook women for men 19% of the time and misidentified darker-skinned women for men 31% of the time. Cade Metz and Natasha Singer, *A.I. Experts Question Amazon's Facial-Recognition Technology*, NEW YORK TIMES, Apr. 3, 2019, https://www.nytimes.com/2019/04/03/technology/amazon-facial-recognition-technology.html?module=inline.

[82] *See e.g.*, Matthew Gault, *Facial Recognition Software Regularly Misgenders Trans People*, VICE, Feb. 19, 2019, https://www.vice.com/en_us/article/7xnwed/facial-recognition-software-regularly-misgenders-trans-people.

[83] Karen Hao, *AI is sending people to jail—and getting it wrong*, MIT TECHNOLOGY REVIEW, Jan. 21, 2019, https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/.

[84] Statement of Clare Garvie Senior Associate, Center on Privacy & Technology at Georgetown Law, Before the U.S. House of Representatives Committee on Oversight and Reform, Hearing on Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties at 13 (May 22, 2019), https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-GarvieC-20190522.pdf.

[85] *Id.* at 14.

[86] ICE has used facial-recognition technology to search license photograph databases maintained in at least two state for purposes of immigration enforcement. Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, NY TIMES, Jul. 7, 2019, https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

[87] According to the U.S. Government Accountability Office, since 2011, the FDA has logged more than 390,000 facial-recognition searches of federal and local databases, including state DMV databases. Statement of Gretta L. Goodwin, Director Homeland Security and Justice, Before the U.S. House of Representatives Committee on Oversight and Reform, *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains* at 6, June 4, 2019, https://www.gao.gov/assets/700/699489.pdf.

[88] *See* Fernandez, *supra* at note 58 (noting that ALPRs have an error rate of at least 10%).

Risk of Data Breach

In addition to intentional or accidental disclosure to law enforcement, data collected in connection with congestion pricing will be at risk of disclosure through hacking and other similar security breaches. For example, in early June 2019, U.S. Customs and Border Protection ("CBP") announced that photographs of travelers and license plates collected at a U.S. border point had been hacked.[89] CBP uses ALPR technology supplied by contractors to detect individuals entering the country without authorization. License plates are recorded and checked against databases maintained by the Department of Homeland Security. CBP stated that the contractor involved in the breach had transferred copies of images collected at a border point to its company network. Although CPB did not publicly name the contractor, Perceptics—the same company that met with the TBTA in February—has been named in the press as the entity involved in the breach.[90] Without a full understanding of the partner agencies and contractors that will receive data collected through congestion pricing in New York City, it is impossible to assess the full scope of the security risk, which grows every time a new entity obtains access.

[89] *See*, *e.g.*, Sidney Fussell, *This is Exactly What Privacy Experts Said Would Happen: CBP's Trove of Biometric Data is Catnip for Bad Actors*, THE ATLANTIC (Jun. 11, 2019), https://www.theatlantic.com/technology/archive/2019/06/travelers-images-stolen-attack-cbp/591403/

[90] Perceptics reportedly has billed itself as the sole provider of ALPR "for passenger vehicle primary inspection lanes at all land border ports of entry in the United States, Canada and at the most critical lanes in Mexico." ASSOCIATED PRESS, *Customs Says Hack Exposed Traveler and License Plate Images*, CNBC, Jun. 11, 2019, https://www.cnbc.com/2019/06/11/us-customs-says-traveler-images-exposed-in-cyberattack.html. CPB reportedly since has attempted to sever its relationship with Perceptics. *See* Geneva Sands, *Customs and Border Protection attempts to end business with contractor involved in data breach*, CNN, July 3, 2019, https://www.cnn.com/2019/07/02/politics/cbp-contractor-data-breach/index.html.

Part 3: Existing Legal Framework

Will Federal or State Privacy Laws Protect Information Collected for Congestion Pricing in New York City?

On the federal level, there is no generally applicable law protecting individuals' privacy interests in information such as their location data, though there are efforts to enact such legislation. Rather, federal law protects individual privacy as to certain subsets of personal information held by certain entities, such as health care providers and financial institutions.[91] Indeed, even if Congress enacts sweeping consumer privacy protections, it is not clear how a federal privacy law might apply to data collected by a public agency such as the TBTA.

In the absence of applicable federal law, several states have enacted legislation specifically governing the use of ALPR technologies, including the retention of data collected through ALPR.[92] However, New York State does not yet have an ALPR law on the books, nor does it have a general privacy law that would govern the collection of data by the TBTA for its tolling program.[93] Thus far, efforts to enact legislation in New York State that would safeguard location information have not been successful and, even if passed, likely would not apply to data collected by the City's tolling program.[94] Although there is growing support for local efforts to establish legislative oversight of NYPD's surveillance techniques, proposed local legislation would apply only to surveillance by NYPD and, as currently drafted, would not extend to other City agencies.[95] That said, in July 2019, Governor Cuomo signed a bill establishing a state-wide task force to study, among other things, current state laws addressing AI, criminal and civil

[91] *See, e.g.,* 45 C.F.R. Parts 160, 162, and 164; Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338, codified in relevant part primarily at 15 U.S.C. §§ 6801-6809, §§ 6821-6827.

[92] *See*, *e.g.*, Calif. Veh. Code § 2413 (prohibits California Highway Patrol from selling or making available ALPR data to third parties, requires deletion of retaining ALPR data after 60 days (except where such data is being used as evidence or in felony investigations), and requires internal monitoring systems to prevent unauthorized uses of ALPR). For a summary of state ALPR laws, *see* National Conference of State Legislatures, Automated License Plate Readers: State Statutes (Mar. 15, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx.

[93] *Id.*

[94] For example, a comprehensive privacy bill pursuant to which historic or real-time geolocation data would be classified as protected information applied only to businesses, and expressly exempted state and local governments from the scope of the bill. *See* New York Privacy Act, 2019 N.Y. S.B. 5642, § 1101(2), https://legislation.nysenate.gov/pdf/bills/2019/S5642. Similarly, it is not clear whether a draft bill proposing to limit law enforcement access to electronic device information, such as location information, would apply to data collected by the City in connection with the tolling program, as the bill appears to have been aimed at protecting against unlawful search and seizure of devices owned by individuals, rather than equipment installed to implement a government program. *See* 2019 N.Y. S.B. 4619, https://legislation.nysenate.gov/pdf/bills/2019/S4619.

[95] *See* New York City Council, Int. No. 487, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0&Options=ID%7cText%7c&Search=The+Public+Oversight+of+Surveillance+Technology (proposing a law to "amend the administrative code of the city of New York, in relation to creating comprehensive reporting and oversight of NYPD surveillance technologies").

liability for violations of law caused by entities equipped with AI, and public sector applications of AI and cognitive technologies.[96] The task force must issue a report regarding its findings no later than December 1, 2020.[97] Thus, while it is possible that New York ultimately will enact laws restricting the way in which law enforcement might use AI to mine data collected through the City's congestion pricing program, no such law yet exists.[98]

Does the Fourth Amendment Prevent Law Enforcement From Accessing Information Collected for Congestion Pricing in New York City?

The Fourth Amendment of the U.S. Constitution prohibits law enforcement from conducting unreasonable searches and seizures. Although the Supreme Court has interpreted the Fourth Amendment to limit the ability of law enforcement to track individuals without a warrant under certain circumstances, it has not directly addressed the specific question of location data collected through the use of ALPR technology. However, two recent Supreme Court cases provide insight into how the Fourth Amendment may apply to the collection and use of information gathered through ALPR (or similar) technology used to implement a zone-based pricing plan.

In 2012, the Supreme Court held in *United States v. Jones* that the Fourth Amendment limits law enforcement's ability to track an individual's movements through a GPS tracker attached to a private vehicle without having first obtained a search warrant by demonstrating probable cause.[99] This holding was limited to the physical attachment of a tracking device to a vehicle—the Court did not conclude that location monitoring using traditional surveillance technologies, such as roadside cameras, constitutes a Fourth Amendment search.[100]

[96] *See* 2019 N.Y. S.B. 3971 § 1, https://www.nysenate.gov/legislation/bills/2019/s3971.

[97] *Id.* at § 5.

[98] In 2017, the City enacted legislation establishing the New York City Automated Decision Systems ("ADS") Task Force to make recommendations regarding the use of AI algorithms by City agencies and offices and to develop procedures, *inter alia*, to determine whether AI-based decisions have discriminatory effects. New York City Council, Int. No. 1696, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0. Since its establishment, the ADS Task Force has been "starved for support" and unable to take the necessary actions to fulfill its purpose due to a lack of transparency from the City. Albert Fox Cahn, *The Irony Behind de Blasio's Proposed Robot Tax*, Daily News, Sept. 11, 2019, https://www.nydailynews.com/opinion/ny-oped-the-irony-behind-de-blasios-proposed-robot-tax-20190911-6fwkugtgbfavrp7zkn7u6odeca-story.html; Colin Lecher, *New York City's Algorithm Task force Is Fracturing*, The Verge, Apr. 15, 2019, https://www.theverge.com/2019/4/15/18309437/new-york-city-accountability-task-force-law-algorithm-transparency-automation.

[99] *United States v. Jones*, 565 U.S. 400 (2012) (holding that the attachment of a GPS tracking device to a vehicle and use of that device to monitor the vehicle's movements was a search within the meaning of the Fourth Amendment).

[100] In a concurring opinion, Justice Sotomayor has suggested that monitoring an individual's movements absent physical intrusion onto a vehicle (the installation of a tracking device) such as "by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones" may constitute a Fourth Amendment search. *Jones*, 565 U.S. at 415. Sotomayor explained that in "considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements," she would "ask whether people reasonably expect

Six years later, in 2018, the Court built upon its holding in *Jones* and held in *Carpenter v. United States* that the collection of vast amounts of location information from a cell phone service provider constitutes a search under the Fourth Amendment.[101] The Court explained that use of cell phone location data by law enforcement to reconstruct an individual's movements retrospectively contravened the defendant's "reasonable expectation of privacy in the whole of his physical movements."[102] In reaching its decision, the Court rejected arguments that the voluntary provision of location information to a wireless carrier undermines an individual's expectation of privacy, stating that "in no meaningful sense does the [cell phone] user voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements" when choosing to use a cell phone.[103] As was the case in *Jones*, however, the Court's decision in *Carpenter* does not address traditional surveillance technologies.[104] The *Carpenter* Court limited its holding to cell phone technology, but the logic of the ruling leaves open the possibility of future challenges to the use of data collected through ALPR technology.[105]

Depending on the extent of data collected and maintained through the use of congestion pricing, it is possible that the use of such information by law enforcement could be deemed to constitute a search under the Fourth Amendment. Like the cell phone location information in *Carpenter*, data collected from ALPR technology could be used to retrace the movements of an individual over months at a time. If GPS navigation technology or app-based location data is used to implement the congestion pricing plan, the concerns raised in *Jones* may come into play. Accordingly, in planning for the use and disclosure of data collected through congestion pricing, the TBTA must seek to protect drivers' Fourth Amendment rights by only disclosing data to law enforcement when a lawful search warrant has first been obtained. In addition, in deciding how data may be used or disclosed, the TBTA should also take into account the protections offered by the New York State Constitution, which offers greater protections than the U.S. Constitution, particularly with respect to search and seizure law.[106]

that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *Id.* at 416.

[101] *Carpenter*, 138 S.Ct. 2206 (holding that law enforcement's collection of cell-site location information ("CSLI") revealing the location of the defendant's cell phone whenever it made or received calls over a period of 127 days constituted a Fourth Amendment search). In reaching its holding, the Court noted that "[m]uch like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." *Id.* at 2216.

[102] *Id.* at 2219.

[103] *Id.* at 2220 (quoting *Smith v. Maryland*, 442 U.S. 735, 745 (1979)) (internal quotation marks omitted).

[104] *Id.* ("We do not express a view on matters not before us: real-time CSLI . . . We do not . . . call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information.").

[105] *See*, *e.g.*, ELECTRONIC FRONTIER FOUNDATION, *How to Challenge ALPR Searches: Landmark* Carpenter *Decision Changes the Game*, https://www.eff.org/criminaldefender/alpr/how-to-challenge.

[106] *See* N.Y. CONST. art. I, § 12 (protecting against "unreasonable interception of telephone and telegraph communications"). *See also*, Scott N. Fein and Andrew B. Ayers, Protections in the New York State Constitution

Part 4: Recommendations and Best Practices

The forgoing research implicates numerous congestion pricing design choices, necessitating technical and legal safeguards, but none of these concerns should prove fatal to congestion pricing itself. Rather than questioning the validity of congestion pricing as a public policy aim, this work raises questions about how congestion pricing can be structured to provide the desired tolling infrastructure with minimal adverse impacts on marginalized communities and overall privacy.

Given the privacy risks associated with ALPR technology, and the lack of a clear legal framework for protecting individual privacy rights in this context, it is imperative that the TBTA take a privacy-by-design approach to implementing congestion pricing in New York City. Privacy-by-design involves several aspects: *first*, the TBTA should prioritize approaches that do not involve facial recognition, ALPR-enabled cameras, or other technologies that pose an undue privacy risk; *second*, the selected technologies must be implemented in the least-intrusive means possible; and *third*, it is essential that the TBTA adopt policies and procedures designed to protect individuals' privacy in the data collected in connection with congestion pricing.

The TBTA Should Evaluate Alternatives to ALPR-Enabled Cameras, Facial Recognition or Other Technologies that Pose an Undue Privacy Risk

ALPR-Enabled Cameras. To date, cities utilizing congestion pricing schemes have relied upon ALPR technologies as a critical component of their systems. From a privacy perspective, however, ALPR technologies are problematic because ALPR often collects information well beyond that needed to collect a toll from a vehicle entering the CBD, and such information can be used to identify travel patterns, connect individual persons with license plate numbers, and develop profiles based upon travel locations.[107] In light of the privacy risks associated with ALPR, the TBTA should evaluate options that do not involve use of a network of ALPR-enabled cameras or other systems that rely on video or photographs to implement and enforce congestion pricing.[108] In the event that ALPR-enabled cameras are deployed, the TBTA should, at a minimum, implement safeguards that are as privacy protective as those used in Stockholm.

Beyond the Federal Bill of Rights p. 14-16, Albany Law Sch., Apr. 18, 2017, https://www.albanylaw.edu/centers/government-law-center/about/publications/SiteAssets/Pages/defaullt/Pamphlet%20Master%20-%20corrected%207-13-2018%20with%20cover.pdf (providing examples of protections against unreasonable searches and seizures that go beyond the U.S. Constitution).

[107] *See supra* at Part 2.

[108] *See*, *e.g.*, Robin Chase, *The Technology That Could Transform Congestion Pricing*, CityLab, May 8, 2019, https://www.citylab.com/perspective/2019/05/congestion-pricing-technology-apps-road-tolls-data-privacy/589006/ (suggesting that the City adopt a market-based approach whereby the City establish the baseline requirements for private sector apps designed to collect congestion-based fees, and rely on license plate spot-checking for enforcement). *See also* Andrew J. Blumberg and Robin Chase, *Congestion Pricing that Respects "Driver Privacy,"* https://web.ma.utexas.edu/users/blumberg/congestion.pdf (proposing a protocol based upon a blind signature scheme whereby transponders installed in vehicles are assigned "license plate" numbers on a dynamic basis. such numbers are recorded when vehicles enters a congestion-based pricing zone, and the amount

Facial Recognition/AI. Over the past several months, the MTA has begun to test the use of facial recognition technologies at several bridges and tunnels in the City.[109] According to initial reports, the technology did not identify a single face within acceptable parameters, but the MTA reportedly continued the pilot program nevertheless.[110] This experience illustrates the unreliable nature of facial recognition software, which, as explained above, has been proven to have a discriminatory impact. There is simply no need to use facial recognition software for a congestion pricing program, which requires only the collection of a toll, a task that can be accomplished without any biometric information whatsoever. Similarly, congestion pricing can be implemented without the use of machine-learning algorithms designed to recognize a vehicle based upon a set of defined inputs wholly unrelated to toll assessment and collection.

Other Technologies. Similar to ALPR, other technologies under consideration by the TBTA threaten individuals' privacy. For example, in March 2019, the TBTA stated that it was conducting proof of concept demonstrations to examine technologies such as GPS or the use of roadside equipment designed to interface with in-vehicle infotainment systems, smartphone applications, or connected vehicle technologies.[111] The use of these technologies (and other systems, such as cellular networks, small cell [e.g., pico-cell] networks, mesh networks, etc.) is particularly concerning given that many of these technologies are capable of tracking a vehicle's location to a high degree of accuracy.[112] As with data collected through ALPR, data collected by these technologies can be used to track the movement of individuals in the absence of appropriate safeguards. Such technologies must only be implemented with strict legal safeguards that prevent the transformation of congestion pricing into a generalized tracking system. The type and extent of such safeguards will always vary with the tracking capabilities of the specific technology that is deployed. The TBTA must choose those technologies that provide the least persistent, least granular information collection possible to achieve the purpose of the congestion pricing program. It's also important that such tracking be limited to the single data point of when vehicles enter the congestion zone, avoiding driver and passenger–level tracking.

Congestion Pricing Technologies Selected Must be Implemented in the Least Intrusive Means Possible

Any congestion pricing technology ultimately adopted by the TBTA must be implemented so as to minimize the risk of intrusion on individual's privacy. This is particularly the case if New York City's congestion pricing system relies on cameras equipped with ALPR or any other technology that captures videos, photographs, or other imagery and information that

owed is calculated without reference to the vehicles actual license plate number); https://web.ma.utexas.edu/users/blumberg/automated-enforcement.pdf (same).

[109] Paul Berger, *MTA's Initial Foray Into Facial Recognition at High Speed Is a Bust*, THE WALL STREET JOURNAL, Apr. 7, 2019, https://www.wsj.com/articles/mtas-initial-foray-into-facial-recognition-at-high-speed-is-a-bust-11554642000.

[110] *Id.*

[111] March RFP, *supra* note 59.

[112] *See, e.g.,* FHA Technology Primer *supra* note 6 at 12.

can be used to target a vehicle's location or otherwise identify or track the movement of individuals—data that is unnecessary to collect a congestion pricing toll. At a minimum, the TBTA should design congestion pricing with the following principles in mind:

- *Minimize the Types and Amount of Data Collected and Stored*. Every attempt should be made to collect and store only the minimum amount of data required to implement congestion pricing. The TBTA should only collect data necessary to monitor a vehicle's entry into (and, if necessary, exit from) the CBD, and should not collect any data regarding a vehicle's movement within the CBD. In other words, the system should not be designed in any manner that could enable the surveillance or tracking of vehicles or individuals moving within the CBD. If ALPR technology is used, cameras should record license plate numbers only. Cameras should not be used to capture images of a vehicle in full, the vehicle's contents, occupants, or surroundings, or individuals or property within the vicinity of the camera.[113] Any data not directly relevant to the payment and collection of congestion fees should be immediately deleted from databases. Data that is required to collect and enforce fee payments should be retained for the shortest amount of time necessary, and should be immediately deleted after payment has been received.

- *Provide Options to Limit Data Disclosure*. The TBTA should provide drivers with the option to pay congestion-based tolls on an anonymous basis, without revealing their identity.[114]

- *Prohibition Against Building Vehicle Profiles.* It is imperative that the TBTA prohibit the use of any technology that is capable of building unique vehicle "profiles" through the collection and compilation of various data points, such as license plate numbers, type of vehicle (e.g., privately owned or commercial), number of passengers, etc. The creation and maintenance of vehicle profiles to generate travel histories, establish travel patterns, or ascertain likely trip purpose raise significant privacy concerns, as vehicle profiles connect directly to an individual's behaviors and collect information well beyond the scope of congestion pricing.

The TBTA Must Adopt Rules and Procedures Designed to Protect Individual Privacy

In addition to adopting technologies and designing the congestion pricing system in the manner least likely to encroach on individual privacy rights, it is essential that the TBTA also

[113] *See* NYCLU, ACLU OF NEW YORK, *Legislative Memo: Congestion Pricing*, https://www.nyclu.org/en/legislation/legislative-memo-congestion-pricing (recommending privacy protections for inclusion in the 2008 Traffic Mitigation Act).

[114] *See, e.g.*, Recommendation of the Traffic Congestion Mitigation Commission at 73, Jan. 31, 2008, *available at* http://wsj.com/public/resources/documents/TCMC_FINAL_REPORT20080131.pdf?mod=article_inline.

adopt rules and procedures to protect drivers' privacy.[115] These rules and policies should be based upon the following principles:

- *Limits on Use and Disclosure of Data*. All data collected in connection with the congestion pricing plan must be used only for the purpose of collecting toll payments and within the context of drivers' reasonable expectations as to how such data will be used. Data should not be provided to third parties (e.g., credit card companies, insurance companies, marketing companies, etc.) for any purpose. Data should not be shared with law enforcement agencies for intelligence, investigative, or other purposes in real time, and any retrospective requests should only be granted when authorized by a lawful and valid warrant. Data also should not be mined or processed with AI tools. In addition, the TBTA should restrict access to data to only those individuals who have a legitimate need to access such data in order to collect payments or address complaints and disputes, and should implement training programs for such authorized individuals.

- *Consent.* The TBTA should not implement a notice and consent procedure as a means to obtain driver consent to having their data shared with third parties for purposes unrelated to the collection of congestion pricing tolls. Notice and consent procedures typically do not provide a meaningful method by which consumers can make an informed choice. In the context of congestion pricing, the use of notice and consent creates the risk that drivers will inadvertently grant consent without fully understanding the implications of their action.

  If the TBTA does seek driver consent to provide personal information to third parties (other than contractors and vendors engaged by the TBTA to provide technologies and services to implement congestion pricing in the City),[116] it must implement a meaningful opt-in consent procedure. Under an opt-in consent procedure, drivers must be informed as to what data the TBTA collects, how the data is collected, to whom data will be disclosed if consent is provided, and the purposes for which data will be disclosed if consent is provided. Additionally, the TBTA must implement procedures through which drivers could later opt-out of data sharing and inform drivers as to how to exercise that option. Under no circumstances should the TBTA implement a program through which drivers must opt-out to prevent the use and disclosure of their data for purposes unrelated to the implementation of congestion pricing, nor should the TBTA implement a take-it-or-leave it policy, whereby drivers must consent to third-party data disclosure as a condition of driving within the CBD.

- *Data Security*. The TBTA must adopt and maintain security safeguards to protect data from unauthorized access, use, or disclosure, whether accidental or intentional. These safeguards should include, at a minimum, data encryption, multifactor authentication,

[115] Laws adopted by states such as California could provide guidance for these procedures. *See*, *e.g.*, Calif. Civil Code § 1798.90.51.

[116] *See infra* at "Data Security" (recommending safeguards the TBTA should undertake with respect to third-party service providers).

and password protection and should meet or exceed industry standards for the type of data involved. In addition, the TBTA must establish procedures to monitor the congestion pricing system to ensure any data collected is secure. Contractors and vendors engaged by the TBTA to provide technologies and services must be subject to strict contractual obligations to implement security protocols, comply with TBTA-specified data deletion requirements, and undergo periodic training. In addition, the TBTA must implement procedures to audit contractors' compliance with these requirements. Importantly, the TBTA must conduct due diligence of all contractors and vendors before data collection begins to ensure that any such contractors and vendors have appropriate security protocols and will not share or disclose information collected in connection with the tolling program. Finally, before collecting any data, the TBTA must develop a comprehensive plan to respond to data breaches, including, for example, procedures to notify affected parties.

Nevertheless, even if the TBTA takes the above measures, due to the ever-present risk of a security breach, the TBTA must minimize the amount of data that is collected through the congestion pricing program. Indeed, data that the program has not collected cannot be subject to a breach.

- *Access*. Drivers should be permitted to access records regarding any data the congestion system collects and maintains on an individualized basis. The TBTA should maintain records regarding the use, access, and disclosure of collected data and provide such records to drivers upon request. At a minimum, drivers should be provided information regarding access to their data, including details regarding by whom the data was accessed and the reason for such access.

- *Transparency*. All policies and procedures regarding the collection, storage, retention, deletion, access, and use of data collected by the congestion pricing system should be made available to the public. At a minimum, these policies should describe (1) the purposes for which data will be collected and used by the TBTA and the City; (2) security safeguards, including information on how the security of the congestion pricing system will be monitored; (3) data retention and destruction policies; (4) the circumstances under which data may be used, accessed, shared with any third party, including law enforcement; and (5) drivers' rights to access data.

- *Accountability*. The TBTA should implement procedures designed to ensure compliance with all rules, policies, and procedures governing the collection, use, disclosure, and retention of congestion pricing data. These procedures could include periodic internal audits but also should provide for annual audits by an independent party.

Surveillance Technology
Oversight Project, Inc.

40 Rector Street
9th Floor
New York, NY, 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT

ENGELBERG CENTER
on Innovation Law & Policy
NYU School of Law