

Before the
Office of Maryland Attorney General Anthony G. Brown
Baltimore, MD 21202

In the Matter of

Consumer Complaint Regarding
Violations of Maryland Privacy Law by
Multiple Actors in the Data Industry

We Are CASA

Center for Democracy & Technology

Center on Privacy & Technology at Georgetown Law

Consumer Federation of America

Council on American-Islamic Relations

Demand Progress Education Fund

Electronic Frontier Foundation

Electronic Privacy Information Center

Fight for the Future

Surveillance Technology Oversight Project

via electronic filing

August 19, 2026

Laura M. Moy
Technology Law Clinic
Georgetown University Law Center
600 New Jersey Avenue, NW
Washington, DC 20001
(202) 662-9547

Counsel for We Are CASA

TABLE OF CONTENTS

BACKGROUND AND SUMMARY	1
ARGUMENT.....	4
I. Companies violate Maryland privacy law by collecting, processing, sharing, and selling Marylanders' precise geolocation data violates Maryland privacy law.	5
A. Penlink impermissibly collects, processes, shares, and sells Marylanders' precise geolocation data in the form of cellphone location data.....	6
B. Multiple license plate recognition vendors impermissibly collect, process, share, and sell Marylanders' precise geolocation data in the form of vehicle location data.....	10
II. Companies violate Maryland privacy law by selling Marylanders' personal data to immigration enforcement authorities.	18
A. ThunderCat Technology impermissibly sells Marylanders' personal data to immigration enforcement authorities.	18
B. Thomson Reuters impermissibly sells Marylanders' personal data to immigration enforcement authorities.	19
C. LexisNexis impermissibly sells Marylanders' personal data to immigration enforcement authorities.	21
III. Companies violate Maryland privacy law by selling Marylanders' motor vehicle records to immigration enforcement authorities in circumstances not required by the federal Driver's Privacy Protection Act.....	23
A. Thomson Reuters impermissibly sells Marylanders' motor vehicle records to immigration enforcement authorities.	24
B. LexisNexis impermissibly sells Marylanders' motor vehicle records to immigration enforcement authorities.	25
REQUEST FOR RELIEF.....	25
CONCLUSION.....	27

BACKGROUND AND SUMMARY

We Are CASA through its counsel, the Technology Law Clinic at Georgetown University Law Center,¹ along with the Center for Democracy & Technology, Center on Privacy & Technology at Georgetown Law, Consumer Federation of America, Council on American-Islamic Relations, Demand Progress Education Fund, Electronic Frontier Foundation, Electronic Privacy Information Center, Fight for the Future, and Surveillance Technology Oversight Project, respectfully request that Maryland Attorney General Anthony G. Brown investigate and take enforcement action to halt widespread and deeply harmful violations of Maryland privacy law by the data industry.

As Attorney General Brown and 16 other state AGs recently explained in a letter to Congress (“AGs’ letter”), “[t]he consumer datasets compiled, aggregated, analyzed, and sold by tech companies, advertisers, and data brokers disclose personal and highly specific information about individuals, such as commuting routines, family networks, medical treatment, political activity, religious practices, biometrics, and more.” And the scale and scope of the data broker industry are rapidly expanding with technological advances related to artificial intelligence, which enable data brokers to deduce even more details about individuals.²

The wealth of Marylanders’ data that is aggregated and sold is not used only for commercial purposes, but as the AGs’ letter described, it also is used by federal law enforcement agencies for various operations.³ For example, federal agencies have purchased detailed historical location data about individuals’ mobile devices.⁴

Attorney General Brown has been an outspoken defender of Marylanders’ privacy rights in this context, calling on Congress to “close the data-broker loophole” and “require warrants for federal access to Americans’ digital data.”⁵ Maryland is also

¹ Clinical teaching fellows Catherine E. Ferri and Alissa Johnson in the Technology Law Clinic at Georgetown Law provided excellent editing and citation support with this filing.

² Letter from Raúl Torrez et al., to Senate Comm. on Homeland Sec. and Gov’t. Affairs Comm. Mar. 24, 2026) https://oag.maryland.gov/News/Documents/pdfs/2026-03-23%20Domestic%20Surveillance%20Letter_ACTIVEPDF1.pdf [<https://perma.cc/T5HW-7V4C>] [hereinafter AGs’ Letter to Congress].

³ *Id.*

⁴ *Id.*

⁵ *Attorney General Brown Calls on Congress to Close Loophole Enabling Federal Mass Surveillance of Americans*, Maryland.gov (Mar. 25, 2026) <https://oag.maryland.gov/News/Pages/Attorney-General-Brown-Calls-on-Congress-to-Close-Loophole-Enabling-Federal-Mass-Surveillance-of-Americans.aspx> [<https://perma.cc/MRW8-HLYG>]. The Attorney General also recently joined a multistate lawsuit against the Trump Administration for “trying to unlawfully seize Marylanders’ personal data with no legitimate purpose, no safeguards to protect it, and no warning to the public or consultation with the states.”

among the nation’s leading states in trying to rein in these practices through legislation. In 2024, Maryland passed the Maryland Online Data Privacy Act (MODPA). This year, Maryland passed the Maryland Data Privacy Act of 2026, which went into effect on July 1, 2026. As those laws make clear, data brokers may not:

- Collect, process, or share Marylanders’ sensitive data, including location data, except as strictly necessary to deliver a product or service requested by the consumer; or
- Sell Marylanders’ sensitive data, including location data.

In addition, previously overbroad exceptions to Maryland privacy laws – which some data brokers may have relied upon to justify widespread sale of Marylanders’ private information – have been tightened under new provisions included in the 2026 law that took effect this month. Specifically:

- An exception to Maryland privacy law that permits the sharing of information with law enforcement no longer extends to mere “inquiries” or “investigations” without some kind of legal process like a subpoena;
- An exception that permits companies to sell information they get from government records now only applies if those same companies also abide by any restrictions that the government placed on their use of the records when it shared those records; and
- An exception that permits the sharing of Marylanders’ motor vehicle records now only applies when the federal Driver’s Privacy Protection Act of 1994 requires that information to be shared.

As this Consumer Complaint explains, existing practices in the data industry violate Marylanders’ privacy rights and these modest, commonsense provisions in Maryland privacy law. These practices not only constitute ongoing violations of Maryland law, they also are deeply harmful. The data industry fuels predatory advertising and outright scams, increases vulnerability to data breaches of sensitive financial details, and facilitates stalking and harassment.

Attorney General Brown Sues Trump Administration for Unlawfully Demanding Personal Information of CDL Drivers, Maryland.gov (Aug. 13, 2026), <https://oag.maryland.gov/News/pages/Attorney-General-Brown-Sues-Trump-Administration-for-Unlawfully-Demanding-Personal-Information-of-CDL-Drivers.aspx> [<https://perma.cc/W32X-RQU2>].

The data industry is also complicit in law enforcement agencies' circumvention of Marylanders' constitutional rights, by enabling federal, state, and local law enforcement to simply purchase privacy-invasive information rather than going to court for a warrant as the Constitution contemplates. Because the data industry makes one-stop-shopping for detailed and sensitive information so easy, law enforcement agencies increasingly turn to this industry for seamless access to a wealth of information, rather than following legal process.⁶

If these practices are allowed to proceed, federal agencies will effectively be able to circumvent constitutional limits and judicial oversight altogether, and to conduct dragnet searches and go on fishing expeditions through Marylanders' private lives in ways that they should not be able to do. For example, as this Consumer Complaint describes, federal immigration authorities are known heavy users of commercial data services, which help them identify neighborhoods and individuals to target for enforcement operations that break up Maryland families and devastate communities.

Unfortunately, the federal Congress has not acted on the call from Attorney General Brown and 16 other state AGs to "stop the federal government's ability to evade existing legal limits on mass surveillance through the data broker loophole."⁷ Fortunately, however, the Maryland legislature has.

Complainants urge Attorney General Brown to use the full force of Maryland's strong privacy laws and take immediate action to rein in agencies' use of commercially purchased data that enables mass surveillance of Americans without judicial, legislative, or public oversight. Specifically, we call on Attorney General Brown to bring enforcement actions to halt the data industry practices described in this Consumer Complaint. Not only does the rule of law demand full-throated enforcement of Maryland's strong privacy law, but if Marylanders' privacy rights are not vindicated, Marylanders may lose trust in government, law enforcement, and other institutions. People are afraid to use services that require them to share data when they have no idea

⁶ AGs' Letter to Congress, *supra* note 2, at 3 ("The federal government's ability to obtain much of this information in the ordinary course typically requires compliance with some legal process, whether through issuance of a subpoena, judicial review through warrant requirements, existence of individualized suspicion, or pre-acquisition public notice and creation of data protection protocols. The data broker loophole to these safeguards allows for the *de facto* deployment of an artificial-intelligence-powered surveillance system, a disturbing escalation of the already unprecedented collection of personal data by public and private actors.").

⁷ *Id.* at 2.

how that data will be used—or worse, when they have reason to believe that it will be used to harm them and their families.

To protect Marylanders' rights, restore Marylanders' trust in government and other critical institutions, and rein in widespread harmful violations of Marylanders' privacy, we urge Attorney General Brown to investigate and initiate enforcement actions against:

- Penlink, for its practice of selling Marylanders' phone location data in violation of Maryland privacy law;
- Motorola, Thomson Reuters, Insight LPR, LexisNexis, Flock, and others, for their practice of collecting, processing, sharing, and selling Marylanders' vehicle location data in violation of Maryland privacy law;
- ThunderCat Technology, Thomson Reuters, and LexisNexis, for their practice of selling Marylanders' personal data to immigration enforcement agencies in violation of Maryland law; and
- Thomson Reuters and LexisNexis, for their practice of selling Marylanders' motor vehicle records to immigration enforcement agencies in violation of Maryland law.

These practices violate Marylanders' rights and Maryland law, and harm Marylanders as long as they are permitted to continue.

ARGUMENT

The many parties named in this Consumer Complaint violate Maryland law in several ways, representing widespread harmful violations of Marylanders' privacy rights. First, several companies violate Maryland privacy law by collecting, processing, sharing, and selling Marylanders' location data, including the locations of Marylanders' vehicles and mobile devices. This constitutes sensitive data, of which Maryland law prohibits the sale. Second, a number of companies also violate Maryland privacy law by selling or otherwise sharing Marylanders' personal data with immigration enforcement authorities in the absence of a judicial warrant. Third, at least two companies also violate Maryland privacy law by sharing Marylanders' motor vehicle records in circumstances not required by the federal Driver's Privacy Protection Act.

I. Companies violate Maryland privacy law by collecting, processing, sharing, and selling Marylanders' precise geolocation data violates Maryland privacy law.

Multiple companies violate Maryland privacy law by collecting, processing, sharing, and selling location data pertaining to Marylanders' mobile devices and vehicles. Maryland law prohibits data "controllers" from certain behaviors related to "sensitive data." A "controller" is "a person that, alone or jointly with others, determines the purpose and means of processing personal data."⁸ Controllers may not collect, process, or share "sensitive data" "[e]xcept where the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains."⁹ "Process" is defined as "an operation or set of operations performed by manual or automated means on personal data," and "includes collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data."¹⁰ Controllers also may not sell "sensitive data."¹¹ "Sale" is any "exchange of personal data by a controller, a processor, or an affiliate of a controller or processor [sic] to a third party for monetary or other valuable consideration."¹²

Mobile device and vehicle location data vendors violate these provisions of Maryland law by processing, sharing, and selling "sensitive data," in the form of "precise geolocation data,"¹³ which is "information derived from technology that can precisely and accurately identify, within a radius of 1,750 feet, the specific location of a consumer, a mobile device, or a vehicle."¹⁴

⁸ MD Commercial Law Code [hereinafter Commercial Law] § 14-4701(k).

⁹ Commercial Law § 14-4707(a)(1).

¹⁰ Commercial Law § 14-4701(y). The law does not define "collect" or "share."

¹¹ Commercial Law § 14-4707(a)(2) ("A controller may not . . . Sell sensitive data"); Commercial Law § 14-4701(ff) ("Sale of personal data' means the exchange of personal data by a controller, a processor, or an affiliate of a controller or processor [sic] to a third party for monetary or other valuable consideration.").

¹² Commercial Law § 14-4701(ff)(1).

¹³ Commercial Law § 14-4701(gg)(4).

¹⁴ Commercial Law § 14-4701(x)(1); H.B. 711, 2026 Leg., Reg. Sess. (Md. 2026) [hereinafter HB 711] (revising this definition to clarify that the location of a mobile device or a vehicle constitutes precise geolocation data).

A. Penlink impermissibly collects, processes, shares, and sells

Marylanders' precise geolocation data in the form of cellphone location data.

Commercial location data broker Penlink collects, processes, shares, and sells precise geolocation data, and thus violates Maryland law. Indeed, Penlink openly boasts its wealth of location data assets. Penlink's own website describes Penlink's ability to "bring . . . into a single view" a variety of "valuable location data" from consumers' vehicle history, rental car travel history, food delivery and rideshare services, fitness trackers and wearables, family safety apps, and "connected gadgets" such as Bluetooth tags.¹⁵

Penlink's product Webloc offers particularly detailed location data. As explained by journalist Joseph Cox of *404 Media* upon reviewing Webloc-related material,

The material shows Webloc users can search its databases of mobile phone data in various ways. Users can perform a single perimeter analysis to search a specific area for mobile phones across a certain time period. They can draw the target area with a rectangle, circle, or polygon. They then select the maximum number of results the system should display, and the maximum number of devices to return.

Once a Webloc user has identified a device of interest, they can get more details about that particular phone, and, by extension, its owner, by seeing where else it has travelled both locally and across the country. Users can click a route feature which shows the path the device took. The material suggests that if users look at where the device was located at night, they might find the person's possible home, and during the day, the person's possible employer.

The software can also do a multi-perimeter analysis, which monitors multiple locations at once to see which devices have been present at two or more specific places.

¹⁵ Penlink, *6 Overlooked Sources of Tracker Data Investigators Shouldn't Miss*, Aug. 19, 2025, <https://www.penlink.com/blog/6-overlooked-sources-of-tracker-data-investigators-shouldnt-miss/> [<https://perma.cc/ND4W-3P6D>].

A results page then displays the list of discovered devices. This includes whether the phone is an Android or iOS device; the number of days the device visited a given location; the average amount of time a device stayed at the location; and the total number of pieces of location data for that phone.¹⁶

In addition, according to a volume of documents from the past several years obtained and reviewed by researchers at Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, “Webloc provides access to a constantly updated stream of geolocation records from 500 million phones and other mobile devices from across the globe.”¹⁷ Demonstrating the detailed nature of the data, a screenshot provided in a Webloc proposal prepared for the El Salvador National Civil Police shows (as described by Citizen Lab):

[T]he system tracked a male person currently located in Abu Dhabi, who has 141 apps installed on his mobile phone, some of which sent 81 different GPS location coordinates to the system over the past five days. In addition, he was apparently located based on Wi-Fi access points nearby his phone 110 times. The activity graph on the right bottom indicates that the system tracked his location up to 12 times a day.¹⁸

The individualized location data to which Penlink provides access plainly meets Maryland’s definition of “precise geolocation data.” Reporting by both Joseph Cox and the Citizen Lab team indicates that a user is able to view detailed location data derived from a mobile device upon searching by advertising and/or device identifier, or by location perimeters (a search in which, for example, a user might search for devices that have visited both defined location A and defined location B to find the device of a specific target known to have visited both locations).¹⁹ Penlink actively markets the

¹⁶ Joseph Cox, *Inside ICE’s Tool to Monitor Phones in Entire Neighborhoods*, 404 Media (Jan. 8, 2026), <https://www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/> [https://archive.ph/HYbBG].

¹⁷ Wolfie Christl et al., *Uncovering Webloc: An Analysis of Penlink’s Ad-based Geolocation Surveillance Tech*, CitizenLab (Apr. 9, 2026), <https://citizenlab.ca/research/analysis-of-penlinks-ad-based-geolocation-surveillance-tech/> [https://perma.cc/3ETM-APXM].

¹⁸ *Id.*

¹⁹ Joseph Cox, *Inside ICE’s Tool to Monitor Phones in Entire Neighborhoods*, 404 Media (Jan. 8, 2026), <https://www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/> [https://archive.ph/HYbBG].

capability of this data to identify, locate, and study specific individuals.²⁰ The detailed location data sold in the Webloc product therefore would easily constitute “precise geolocation data” within the meaning of Maryland privacy law.²¹

Not only does Webloc location data constitute “sensitive data” within the meaning of Maryland law, but it almost certainly includes *Marylanders’* sensitive data. Penlink has multiple customers for its geolocation products in the state of Maryland.²²

(“The Webloc material says users can filter devices by their unique Apple and Android advertising identifiers, which are often collected by surveillance companies. The material also says users can filter location data by GPS, WiFi, or IP address.”); Christl et al., *supra* note 17. (“Webloc customers can start a surveillance operation by searching for mobile devices that were present in a certain area, which is referred to as a ‘perimeter’ or ‘geofence.’ They can also identify devices that were located in two or more defined areas within a certain period of time, indicating persons travelling from one place to another, according to the El Salvador document.”).

²⁰ EyeTech Solutions, *Propuesta Técnica: Plataforma Avanzada para Recopilar Información Pública, Correlacionar Datos y Procesarlos*, 19 (Feb. 2021), https://citizenlab.ca/wp-content/uploads/2026/04/Eyetechnical_Cobwebs_Technical_Proposal_2021_reproduced.pdf [<https://perma.cc/LH75-6R32>] (Webloc document prepared for El Salvador National Civil Police as obtained and reproduced by Citizen Lab) (“La información del dispositivo recopilada en este proceso es vital para conectar la identificación a la persona real que posee el dispositivo.” English translation: “The information of the device compiled in this process is vital to connect the [device] identification to the real person that possesses the device.”).

²¹ This clearly meets the old definition that was established by the 2024 passage of MODPA and that went into effect in October 2025: “information derived from technology that can precisely and accurately identify the *specific location of a consumer* within a radius of 1,750 feet.” It even more clearly meets the recently updated and clarified definition that explicitly includes “location of a consumer, a mobile device, or a vehicle,” established by the Maryland Data Privacy Act of 2026, which went into effect on July 1, 2026. Even when there is no name or phone number associated with location data, individualized location data is among the most easily identified types of data. See, e.g., Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 Scientific Reports 1376 (Mar. 25, 2013), <https://www.nature.com/articles/srep01376> [<https://perma.cc/TN6A-YHVT>] (finding that “in a dataset where the location of an individual is specified hourly and with a spatial resolution equal to that given by the carrier’s antennas, four spatio-temporal points are enough to uniquely identify 95% of the individuals”); Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret*, N.Y. Times (Dec. 18, 2018), <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> [<https://perma.cc/72LB-FFMQ>] (in illustration of the triviality of location data-based identification, journalists analyzing purportedly “anonymous” cellphone location data tracked down a specific teacher based on the fact that she was the only person who made the trip from a specific house to the middle school where she worked each weekday.).

²² On the day on which this Consumer Complaint is filed, the Maryland Board of Public Works is scheduled to consider a proposed updated contract between Penlink and the Maryland State Police. See Board of Public Works Secretary’s Action Agenda for August 19, 2026 Meeting 164, *Maryland.gov* (last visited Aug. 18, 2026) <https://bpw.maryland.gov/MeetingDocs/2026-Aug-19-Agenda.pdf> (seeking approval of contract ID number W00P7600021, explaining that Penlink “helps investigators efficiently organize call records, social media data, geolocation information, and surveillance content,” and that it “supports agencies and task forces funded through the Governor’s Office of Crime Prevention, the Maryland Criminal Intelligence Network (MCIN), and the High Intensity Drug Trafficking Area (HIDTA) Program”); Christl et al., *supra* note 17 (“We consider Baltimore County police a Webloc customer from 2022 to 2024 and a potential Webloc customer for the entire period from 2020 to 2027.”); see also Baltimore

Such a contract would be of little to no value to a Maryland customer if it did not include data regarding locations in Maryland.

To provide the services associated with Webloc, Penlink collects, processes, shares, and sells this sensitive data. According to a sole source justification document from the Department of Homeland Security regarding Penlink software including Webloc, DHS identified Penlink's products to "integrat[e] location data from multiple sources, build[] event timelines for case development and correlat[e] with external events."²³ Discussing consideration of two vendors that DHS evaluated but rejected to meet this need, the justification document states that the rejected platforms did not have "the ability to automatically monitor and analyze location-based data within specified geographic areas," implying that Webloc does have this ability.²⁴ The "integration" of data from multiple sources constitutes "collecting." The analysis performed on location data constitutes a "process," defined as "an operation or set of operations performed by manual or automated means on personal data" including "collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data."²⁵ When location details are shared with Webloc customers, this constitutes "sharing," and likely also constitutes "sale" when the data is provided for "monetary or other valuable consideration," such as the millions of dollars that Penlink's customers pay for its location data products.²⁶

Finally, it is unlikely that Webloc customers seeking Marylanders' location data fall under any of the exceptions to Maryland privacy law. Maryland privacy law permits data controllers to collect, process, and share sensitive data where "strictly necessary to provide or maintain a specific product or service requested by the

County Office of Budget & Finance, *Public Recordation of Announcement of Non-Competitive Awards Charter* Sec. 902(f) (Apr. 12, 2022), <https://www.baltimorecountymd.gov/files/Documents/Auditor/fiscal%20notes%202022/webnotes052622revisedmemo.pdf> [<https://perma.cc/X6SF-LYLV>].

²³ Office of Acquisition Management, *Sole Search Justification: Simplified Procedures for Certain Commercial Items Exceeding SAT, Including Brand Name 1*, U.S. Immigr. and Customs Enf't. (last updated Sept. 30, 2025) <https://www.documentcloud.org/documents/26173900-ice-penlink-location-data/> [<https://perma.cc/UU26-BV2A>].

²⁴ *Id.*

²⁵ Commercial Law § 14-4701(y). The law does not define "collect" or "share."

²⁶ See Thomas Brewster, *Meet The Secretive Surveillance Wizards Helping the FBI and ICE Wiretap Facebook and Google Users*, *Forbes* (Feb. 23, 2022), <https://www.forbes.com/sites/thomasbrewster/2022/02/23/meet-the-secretive-surveillance-wizards-helping-the-fbi-and-ice-wiretap-facebook-and-google-users/> [<https://perma.cc/58MN-4HYD>] ("With \$20 million revenue every year from U.S. government customers such as the Drug Enforcement Administration, the FBI, Immigration Customs Enforcement (ICE) and almost every other law enforcement agency in the federal directory, PenLink enjoys a steady stream of income. That doesn't include its sales to local and state police, where it also does significant business but for which there are no available revenue figures.").

consumer to whom the personal data pertains,”²⁷ but Penlink is a data broker that provides no services requested by the individuals to whom the sensitive location data pertains. Maryland law also contains narrow law enforcement exceptions to allow for the sharing or sale of Marylanders’ sensitive data in limited circumstances involving targeted, legitimate law enforcement activities involving valid legal process;²⁸ however, Webloc is designed for mass surveillance, likely in a number of scenarios where users provide no subpoena, summons, warrant, or other valid order.²⁹ In addition, as reported by journalists and noted in the letter to Congress from AG Brown and 16 other state AGs, Penlink has active contracts with Immigration & Customs Enforcement.³⁰ Under Maryland law, however, such data may only be shared with or sold to civil immigration authorities if the information sharing is necessary to comply with a judicial warrant or is otherwise required by law.³¹

B. Multiple license plate recognition vendors impermissibly collect, process, share, and sell Marylanders’ precise geolocation data in the form of vehicle location data.

Multiple vendors of vehicle location data in the form of automated license plate recognition (LPR) data also collect, process, share, and sell precise geolocation data, and thus violate Maryland privacy law. Among the vendors in violation of Maryland

²⁷ Commercial Law § 14-4707(a)(1).

²⁸ Commercial Law § 14-4712(a); HB 711, *supra* note 14.

²⁹ See AGs’ Letter to Congress, *supra* note 2, at 3 (discussing Penlink, observing that “[i]n recent use cases, DHS has dropped any pretense of seeking pseudonymized datasets for specific, targeted law enforcement activities. Just last year, ICE issued a no-bid contract to a company called Penlink, obtaining licenses to use two of its location tracking systems powered by AI and sourced from millions of data points from commercial data brokers and social media accounts.”).

³⁰ AGs’ Letter to Congress, *supra* note 2, at 3; Joseph Cox, *ICE to Buy Tool that Tracks Locations of Hundreds of Millions of Phones Every Day*, 404 Media, (Sept. 30, 2025), <https://www.404media.co/ice-to-buy-tool-that-tracks-locations-of-hundreds-of-millions-of-phones-every-day/> [<https://archive.ph/RtxxT>]; Joseph Cox, *Inside ICE’s Tool to Monitor Phones in Entire Neighborhoods*, 404 Media (Jan. 8, 2026), <https://www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/> [<https://archive.ph/HYbBG>].

³¹ Commercial Law § 14-4707(a)(2) (prohibiting a controller from selling sensitive data); *id.* as modified by HB 711, *supra* note 14 (additionally prohibiting a controller from “knowingly sell[ing] the personal data of a consumer to a federal, state, or local governmental unit that, within the 6 months that immediately precede the sale of the personal data, has engaged in or supported civil immigration enforcement through the provision of personnel or material resources”); Commercial Law § 14-4712(a) as modified by HB 711 (defining exceptions for law enforcement).

privacy law for these activities are Motorola, Thomson Reuters, Insight LPR, LexisNexis, and Flock.

LPR data clearly constitutes vehicle location data. As explained by the International Association of Chiefs of Police, these systems “typically capture the following information: a contextual photo of the vehicle, an image of the license plate, the geographic coordinates of where the image was captured, and the date and time of the recording.”³² Further, according to a report by the Congressional Research Service, “[LPR] systems catalogue and store information, particularly license plate number, GPS data, and date and time. This data retention can help law enforcement track where vehicles have been over time.”³³ Data containing timestamped license plate numbers with geographic coordinates is “information derived from technology that can precisely and accurately identify, within a radius of 1,750 feet, the specific location of a consumer, a mobile device, or a vehicle” within the plain meaning of this statutory definition.³⁴

LPR vendors are “controllers” of the vehicle location data captured on their networks. Under Maryland law, “[c]ontroller” means a person that, alone or jointly with others, determines the purpose and means of processing personal data.”³⁵ This is the case even if, as some vendors of the services described below may claim, LPR-equipped camera owners, not the vendors, “own” the vehicle location data in question. In such situations LPR vendors continue to determine the purpose and means of processing the vehicle location data associated with LPRs on their network “jointly with” the parties that they claim “own” the data.

As explained above, Maryland privacy law prohibits controllers from collecting, processing, or sharing sensitive data “[e]xcept where the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains.”³⁶ LPR vendors “collect” vehicle location data when they capture it. LPR vendors “process” vehicle location data when they

³² International Association of Chiefs of Police, *Automated License Plate Recognition*, <https://www.theiacp.org/projects/automated-license-plate-recognition> [<https://perma.cc/KB8Z-D88B>] (last visited Aug. 12, 2026).

³³ Congressional Research Service, *Law Enforcement and Technology: Use of Automated License Plate Readers* at 2 (Aug. 19, 2024), https://www.congress.gov/crs_external_products/R/PDF/R48160/R48160.3.pdf [<https://perma.cc/AMQ7-7WYS>] [hereinafter CRS Report].

³⁴ Commercial Law § 14-4701(x)(1); HB (revising this definition to clarify that the location of a mobile device or a vehicle constitutes precise geolocation data).

³⁵ Commercial Law § 14-4701(k).

³⁶ Commercial Law § 14-4707(a)(1).

provide data analysis that enables their customers to search for specific vehicles and trace multiple locations where a vehicle has been spotted over time,³⁷ because these activities constitute “an operation or set of operations . . . by manual or automated means on personal data” including “collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data,” and are not performed to provide a product or service requested by the individual whose vehicle is being tracked.³⁸ LPR vendors “share” vehicle location data when they reveal or transfer it to other parties.

In many instances, activities of LPR vendors also constitute impermissible sale of sensitive data. Maryland’s definition of “sale of personal data” is broad: “the exchange of personal data by a controller, a processor, or an affiliate of a controller or processor [sic] to a third party for monetary or other valuable consideration.”³⁹ When an LPR vendor receives payment from its customers in exchange for vehicle location data, this constitutes a “sale” within the meaning of Maryland law, regardless of whether or not that vendor owns the data at issue.

Finally, like Webloc discussed above, vendors of Marylanders’ vehicle location data are unlikely to fall under exceptions to Maryland privacy law designed to permit the collection, processing, sharing, or sale of Marylanders’ sensitive data in limited circumstances involving targeted, legitimate law enforcement activities involving valid legal process.⁴⁰ Law enforcement uses vehicle location data from these vendors for a variety of activities, which often do not involve any showing of process.⁴¹

³⁷ CRS Report, *supra* note 33, at 2 (“ALPR systems catalogue and store information, particularly license plate number, GPS data, and date and time. This data retention can help law enforcement track where vehicles have been over time.”).

³⁸ Commercial Law § 14-4701(y). The law does not define “collect” or “share.”

³⁹ Commercial Law § 14-4701(ff)(1).

⁴⁰ Commercial Law § 14-4712(a); HB 711, *supra* note 14.

⁴¹ Maryland Coordination and Analysis Center, Administrative Policy: Automated License Plate Recognition Program Standard Operating Procedure, <https://mcac.maryland.gov/wp-content/uploads/2024/05/Automated-License-Plate-Recognition-Program-Standard-Operating-Procedure-5.2.24.pdf> [<https://perma.cc/AR4A-9GJR>] (asserting that LPR data may be used by Maryland agencies for a variety of purposes, including but not limited to “crime analysis,” alerting law enforcement officials that a particular license plate number is on a “hot list” of targeted numbers, or notifying law enforcement officials of the location or travel route of a particular vehicle); *see also* CRS Report, *supra* note 33 (explaining that law enforcement agencies may use LPRs for “a variety of proactive and reactive policing purposes, including gathering intelligence and evidence, helping identify potential suspects, and facilitating crime scene analysis,” acknowledging that “there are no data on its use at various phases of the criminal justice system – from generating investigative leads and helping establish probable cause for an arrest or indictment to serving as evidence in courtrooms.”).

1. Motorola

Motorola collects, processes, shares, and sells vehicle location data derived from its own network in violation of Maryland law. Motorola's Vigilant PlateSearch product provides "patented analytics and billions of license plate scans from your agency's own cameras, other departments cameras, enterprise partners and a nationwide commercial data network to identify, predict and alert to vehicle sightings."⁴² It enables users to "pinpoint past vehicle locations," touting the ability to "[s]cour billions of easily filterable historical vehicle scans using just a license plate number, time, date or location."⁴³ Motorola's product offers not just historical data, but also real-time data and alerts.⁴⁴ Motorola shares commercial LPR data⁴⁵ as well as its customers' LPR data,⁴⁶ and it sells this data when it does so in exchange for payment.⁴⁷

Motorola is a "controller" of this vehicle location data because "alone or jointly with others, [it] determines the purpose and means of processing"⁴⁸ the data. Motorola reserves for itself and its licensors "all title and rights to Commercial LPR Data" integrated into the LPR services it offers,⁴⁹ indicating that it alone determines the purpose and means of processing that data. In addition, although Motorola asserts that

⁴² "Vigilant Platesearch: Transforming License Plate Data Into Promising Leads" at 1, Motorola Solutions (Aug. 2020), https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/reaperhd-mobile-lpr-system/vigilant_platesearch_fact_sheet.pdf [<https://perma.cc/W2V5-WGB8>].

⁴³ *Id.* at 2.

⁴⁴ *Id.*

⁴⁵ See Motorola Solutions, *Managing Your LPR Data* 1 (last visited Aug. 18, 2026), https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/vigilant-vehiclemanager/lpr_data_management_fa_en_us.pdf [<https://perma.cc/7FPQ-SNFG>] ("We maintain a separate database of commercial LPR data. This data is collected by repossession vehicles. . . . We provide our law enforcement and enterprise customers access to this commercial dataset to generate improved vehicle location insights with a greater quantity of data points.").

⁴⁶ As noted below, Motorola participates jointly in making this determination with its customers, including by restricting its customers' ability to share their own LPR data with other parties unless those other parties also subscribe to Motorola services.

⁴⁷ According to Motorola sales materials, Motorola charges thousands to tens of thousands of dollars to provide law enforcement agencies with a subscription to "Commercial LPR Data access," which includes "[a]ccess to all Vigilant commercially acquired national vehicle location data" as well as associated hosting and analytical tools. Pamphlet from VendorLink, Motorola Solutions (last visited Aug. 18, 2026), <https://www.myvendorlink.com/external/vfile?d=vrf&s=190009&v=76606&sv=0&i=28&ft=o> [<https://perma.cc/9UR3-YWRA>].

⁴⁸ Commercial Law § 14-4701(k).

⁴⁹ Motorola Solutions, Inc., *Mobile Video & LPR Addendum* v2.1 7.31.25 at § 4.2.2, https://www.motorolasolutions.com/content/dam/msi/docs/msi-standards_terms-conditions/Mobile-Video-and-LPR-Addendum.pdf [<https://perma.cc/39DZ-FFVV>].

“Customer LPR Data is considered Customer Data . . . subject to the Customer’s own retention policy,” Motorola jointly controls the purpose and means of processing that data by restricting customers’ ability to share that data only to other parties that subscribe to specific Motorola services.⁵⁰

2. Thomson Reuters

Thomson Reuters collects, processes, shares, and sells vehicle location data sourced from Motorola and other commercial partners, in violation of Maryland law.⁵¹ According to a 2023 document prepared by Thomson Reuters for the Baltimore Police Department regarding the Thomson Reuters “CLEAR” product:

Thomson Reuters License Plate Recognition (LPR) utilizes Motorola/Vigilant Solutions live gateway of commercial license plate data to plot vehicle locations within the CLEAR interface. The LPR gateway delivers more than 7 billion commercial results from more than 10 years of license plate data collection, with new license plate scans added at a rate of more than 150 million per month. Multiple tools will give you clues to someone’s location history, activity history, and more. You can even set up alerts to be notified when a vehicle has been recognized.⁵²

Documents that a Thomson Reuters representative sent in 2025 to a customer in Hagerstown, Maryland boasted that the company’s “law enforcement customers have access to more than six (6) million images of vehicles and license plates from a nationwide network of cameras (excluding Hawaii). Images are date/time stamped and

⁵⁰ *Id.* at § 4.2.3 (“Customer has the option to share its Customer LPR Data with LEAs that have a Subscription with Motorola for VehicleManager access. Customers with a Subscription to VME may also share its Customer LPR Data with other non-LEA Customers who have a Subscription with Motorola for VME access. If Customer opts, in its sole discretion, to share its Customer Data with another customer of Motorola, Customer thereby grants to the recipient customer the rights to use such Customer LPR Data in accordance with the terms of VehicleManager or VME, as applicable.”).

⁵¹ Thomson Reuters is a “controller” of the LPR data analyzed and offered via its CLEAR product because it collects that data through commercial transactions and determines the purpose and means of processing that data. *See* Andrea Hoyt et al., Report Prepared by Thomson Reuters CLEAR for Baltimore Police Department 2 (Dec. 1, 2023), <https://boesubmit.baltimorecity.gov/Files/af9f9624-1690-4864-a72b-3cc7e972c3a8.pdf> [<https://perma.cc/VDY9-BHZL>] (marketing “commercial license plate data” (emphasis added) and making no claim or assertion that users of the platform somehow own or control the underlying data themselves); Commercial Law § 14–4701(k) (defining “controller” as “a person that, alone or jointly with others, determines the purpose and means of processing personal data”).

⁵² Hoyt et al., *supra* note 51, at 2.

include geo-coordinate information.”⁵³ Thomson Reuters shares this data with its customers, and it sells this data when it does so in exchange for payment.⁵⁴

A density map illustrating the locations of cameras from which Thomson Reuters CLEAR vehicle data is sourced indicates that vehicle locating cameras are particularly dense in Baltimore.⁵⁵

3. Insight LPR

Insight LPR collects, processes, shares, and sells vehicle location data derived from its own network, in violation of Maryland law.⁵⁶ Insight LPR’s “MX Guardian” product “can enable agencies to securely access commercially generated vehicle intelligence without the cost, complexity, or limitations of deploying traditional, agency-owned ALPR systems.”⁵⁷ The commercial LPR data that Insight LPR offers includes “millions of scans monthly,”⁵⁸ and according to a 2024 press release, “[I]nks over 1,000 Insight LPR communities, including businesses, neighborhoods, and law enforcement agencies.”⁵⁹ MX Guardian’s integrated processing functions enable users

⁵³ Letter from Jon Dubs, Thomson Reuters Account Executive, Public Safety, to Kristy E. Carroll, Hagerstown Police Department (Feb. 14, 2025), <https://hagerstown.novusagenda.com/agendapublic/AttachmentViewer.ashx?AttachmentID=13359&ItemID=13219> [<https://perma.cc/C2YY-VKKG>]; see also Letter from Adam Oehmke, Thomson Reuters Dedicated Renewal Specialist to Brooke Lindemann, Fort Bend County (July 29, 2021), https://agendalink.fortbendcountytexas.gov/mindocs/2021/CCTR/20210810_3535/minutes/3348_31F_signed_contract-thom.reu..pdf [<https://perma.cc/GTY4-PHEF>].

⁵⁴ A proposal submitted to the Hagerstown Police Department in January 2025 quoted a price of \$1,620.02/month for “CLEAR for Law Enforcement – Investigators Plus with LPR (License Plate Recognition)” for up to 100 users. Jon Dubs, Thomson Reuters CLEAR Proposal to Hagerstown Police Department, Thomson Reuters CLEAR (Jan. 30, 2025), <https://hagerstown.novusagenda.com/agendapublic/AttachmentViewer.ashx?AttachmentID=13362&ItemID=13219> [<https://perma.cc/R7AZ-2B7I>].

⁵⁵ *MAS Scan Density Report*, Vigilant VehicleManager (Dec. 1, 2023), <https://boesubmit.baltimorecity.gov/Files/33beebcd-19a9-4dfd-bea6-35e05ff249f6.pdf> [<https://perma.cc/2GXS-NFKY>].

⁵⁶ Insight LPR is a “controller” of the LPR data that it offers because it collects that data through its own network and determines the purpose and means of processing that data. See Commercial Law § 14–4701(k) (defining “controller” as “a person that, alone or jointly with others, determines the purpose and means of processing personal data”).

⁵⁷ *Beyond Fixed Infrastructure: Expanding Investigative Visibility Through Commercial Vehicle Intelligence*, Insight LPR (July 27, 2026), <https://insightlpr.com/2026/07/27/beyond-fixed-infrastructure/> [<https://perma.cc/J72B-PYGL>].

⁵⁸ *Commercial Vehicle Intelligence*, LexisNexis, <https://risk.lexisnexis.com/insights-resources/article/license-plate-reader-lpr-tools-for-investigations> [<https://perma.cc/Z73D-ZDBK>].

⁵⁹ Insight LPR, *Insight LPR Launches MX Guardian Software and Solar-Powered Cameras, Designed by Law Enforcement*, Police 1 (July 30, 2024), <https://www.police1.com/police-products/traffic-enforcement/license-plate-readers/insight-lpr-launches-mx-guardian-software-and-solar-powered-cameras-designed-by-law-enforcement> [<https://perma.cc/2T8V-FETZ>].

to “[e]ffortlessly sort through millions of records and pinpoint vehicles of interest using investigative leads and suspicious activity indicators. MX Guardian proactively alerts [users] upon detection of a hotlist vehicle, enabling prompt intervention.”⁶⁰

4. LexisNexis

LexisNexis collects, processes, shares, and sells vehicle location data sourced from Insight LPR and other commercial partners, in violation of Maryland law.⁶¹ According to a public LexisNexis webpage titled “License Plate Reader (LPR) Data for Investigations” marketing this service, “LexisNexis Risk Solutions now offers agencies access to connected partner solutions, including LPR Tools, through the Accurint Public Safety Marketplace.”⁶² When LexisNexis users subscribe to this data, the associated processing and analysis tools enable them to “expand[] their investigative reach by enhancing commercial vehicle intelligence captured in connected partner solutions with the LexisNexis data assets and linking technology.”⁶³ LexisNexis also sells LPR data to customers as part of bespoke products, such as the system described in a July 2026 contract with Immigration and Customs Enforcement, for which the agency plans to pay nearly \$7 million.⁶⁴

5. Flock

Flock collects, processes, shares, and sells vehicle location data derived from its own network, in violation of Maryland law. Flock’s website advertises it as the “largest

⁶⁰ *MX Guardian*, Insight LPR, <https://insightlpr.com/technology/mx-guardian/> [<https://perma.cc/3X7D-9LH5>].

⁶¹ LexisNexis is a “controller” of the LPR data analyzed and offered via its Accurint product because it collects that data through commercial transactions and determines the purpose and means of processing that data. See Commercial Law § 14–4701(k) (defining “controller” as “a person that, alone or jointly with others, determines the purpose and means of processing personal data”).

⁶² Commercial Vehicle Intelligence, LexisNexis, <https://risk.lexisnexis.com/insights-resources/article/license-plate-reader-lpr-tools-for-investigations> [<https://perma.cc/Z73D-ZDBK>].

⁶³ *Id.*

⁶⁴ See Joseph Cox, *ICE to Pay LexisNexis Millions for Data to Feed to Palantir*, 404 Media (Aug. 10, 2026), <https://www.404media.co/ice-to-pay-lexisnexis-millions-for-data-to-feed-to-palantir/> [<https://archive.ph/OYIRP>]; Performance Work Statement (PWS): Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) Law Enforcement Investigative Database Subscription, 70CMSD26CXXXXXX at 1 (July 22, 2026), <https://www.documentcloud.org/documents/28547603-ice-contract-for-lexisnexis-palantir/> [<https://perma.cc/VT6K-7JM9>] (“ICE requirement of a web-based law enforcement investigative database platform is to . . . integrate investigative capabilities with the license plate recognition capabilities to be utilized by multiple ICE Directorates”).

fixed LPR network” and boasts “billions of monthly plate reads.”⁶⁵ Flock customers include over 5,000 law enforcement agencies, over 6,000 homeowners associations, and over 1,000 businesses.⁶⁶

Flock is a “controller” of this vehicle location data because “jointly with others, [it] determines the purpose and means of processing”⁶⁷ LPR data. Flock asserts that “all right, title, and interest in and to Customer Data belong to and are retained by Customer.”⁶⁸ However, under Flock’s terms and conditions, the customer “grants to Flock a limited, non-exclusive, royalty-free, irrevocable, perpetual, worldwide license to (a) use and disclose Customer Data to provide the Flock Services; and (b) use Customer Data to support and improve Flock’s products and services.”⁶⁹ Flock thus reserves the ability to determine the purpose of processing data captured on its network. In addition, Flock claims the “exclusive right to determine and control the method, timing, format, and medium of such access or delivery [to LPR data], and is not obligated to provide Customer Data in any alternative form, format, or transmission method outside of the Web Interface.”⁷⁰ Flock thus clearly controls the means of processing and sharing data associated with its network.

⁶⁵ *Go Beyond Plates with LPR That Accelerates Cases*, Flock, <https://www.flocksafety.com/products/national-lpr-network> [<https://perma.cc/F82L-CKGV>].

⁶⁶ *Id.*

⁶⁷ Commercial Law § 14-4701(k).

⁶⁸ Flock, Terms and Conditions § 4.1 (Feb. 16, 2026), <https://www.flocksafety.com/legal/terms-and-conditions> [<https://perma.cc/4339-2BNS>]; see *Flock Provides Terms & Conditions Update to Make Definitions Simpler and Provide Customer Clarity*, Flock (Feb. 17, 2026), <https://www.flocksafety.com/blog/flock-provides-terms-conditions-update-to-make-definitions-simpler-and-provide-customer-clarity> [<https://perma.cc/4LB4-YTBR>] (“Customers own and control their data. Flock provides the services.”).

⁶⁹ Flock, Terms and Conditions § 4.1 (Feb. 16, 2026), <https://www.flocksafety.com/legal/terms-and-conditions> [<https://perma.cc/4339-2BNS>].

⁷⁰ *Id.* Flock’s assertion of the “exclusive right” to determine the means of data access and explicit disavowal of any obligation to provide data in any form outside of the Flock platform notably fails to satisfy an important stipulation required of data processors under the European Union’s General Data Protection Regulation, from which the concepts of data “controller” and “processor” likely originated in U.S. state privacy laws: that “at the choice of the controller, [the processor] deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.” Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 28(3)(g), 2016 O.J. (L 119) 1.

6. Unnamed other parties

There likely are a number of other parties that collect, process, share, and sell vehicle location data in violation of Maryland law. A 2025 market survey report on LPRs published by the Department of Homeland Security “identified 16 commercial off-the-shelf systems, all of which offer either a completely integrated ALPR system or an ALPR software-based system that can be integrated with new or existing ALPR hardware.”⁷¹ In addition, the marketing materials of many of the vendors named above indicate that vehicle location data includes “commercial” data from other sources such as parking garages, businesses, and towing companies.

II. Companies violate Maryland privacy law by selling Marylanders’ personal data to immigration enforcement authorities.

Many companies also violate Maryland privacy law because they sell Marylanders’ personal data to entities engaged in civil immigration enforcement activities. Under applicable Maryland law, a data controller may not “knowingly sell the personal data of a consumer to a federal, State, or local governmental unit that, within the 6 months that immediately precede the sale of the personal data, has engaged in or supported civil immigration enforcement through the provision of personnel or material resources.”⁷² “Personal data” is “any information that is linked or can be reasonably linked to an identified or identifiable consumer.”⁷³

A. ThunderCat Technology impermissibly sells Marylanders’ personal data to immigration enforcement authorities.

ThunderCat sells personal data to an agency that engages in civil immigration enforcement in violation of Maryland law. In June 2026, a journalist at *404 Media* reported that ThunderCat Technology, LLC is selling individual taxpayer identification numbers (ITINs) to Homeland Security Investigations (HSI),⁷⁴ one of the three

⁷¹ *Automated License Plate Readers Market Survey Report*, U.S. Department of Homeland Security, National Urban Security Technology Laboratory at v (June 2025), https://www.dhs.gov/sites/default/files/2025-06/25_0606_st_lprmsr.pdf [<https://perma.cc/YC3L-PVLJ>].

⁷² HB 711, *supra* note 14, at p. 6 ¶¶ 4–8 (revising Commercial Law § 14-4707(a)).

⁷³ Commercial Law § 14-4701(w)(1).

⁷⁴ Joseph Cox, *ICE Appears to Be Buying Immigrants’ Tax Identifiers from a Data Broker*, *404 Media* (June 17, 2026), <https://www.404media.co/ice-appears-to-be-buying-immigrants-tax-identifiers-from-a-data-broker/> [<https://archive.ph/vm51q>].

operational directorates of U.S. Immigration and Customs Enforcement.⁷⁵ ITINs plainly constitute personal data under Maryland law because they are “linked or can be reasonably linked to an identified or identifiable consumer” – indeed, their very purpose (as indicated by their name) is to identify discrete individual taxpayers.

In recent months, HSI has engaged in a large volume of civil immigration enforcement actions, as well as provided personnel to support civil immigration enforcement. Although HSI’s primary charge is to “conduct[] federal criminal investigations,”⁷⁶ a recent investigation by a researcher at the Cato Institute revealed that under the Trump administration, thousands of HSI agents have been diverted from their normal work to instead assist civil immigration enforcement.⁷⁷

B. Thomson Reuters impermissibly sells Marylanders’ personal data to immigration enforcement authorities.

In addition to selling Marylanders’ sensitive data in violation of Maryland privacy law, as discussed above, Thomson Reuters also violates Maryland law by selling non-sensitive personal data to an agency that engages in civil immigration enforcement. Specifically, Thomson Reuters provides the Department of Homeland Security with personal data as part of its product called “Consolidated Lead Evaluation and Reporting” (CLEAR).⁷⁸

⁷⁵ U.S. Immigration and Customs Enforcement, <https://www.ice.gov/about-ice> [<https://perma.cc/6A49-RWNE>] (stating that ICE “has an annual budget of approximately \$8 billion, primarily devoted to three operational directorates – Homeland Security Investigations (HSI), Enforcement and Removal Operations (ERO) and Office of the Principal Legal Advisor (OPLA).”).

⁷⁶ *Our Mission – What We Do, How We Do It*, U.S. Immigration and Customs Enforcement, <https://www.ice.gov/hsi/who-we-are> [<https://perma.cc/95Z2-KZZN>].

⁷⁷ David J. Bier, *ICE Has Diverted Over 25,000 Officers from Their Jobs*, Cato at Liberty (Sept. 3, 2025), <https://www.cato.org/blog/ice-has-diverted-over-25000-officers-their-jobs> [<https://perma.cc/3G7X-ZWHQ>]; see Press Release: Hickenlooper, Gallego, Colleagues Call Out Trump Admin for Diverting Federal Agents for Immigration Enforcement, Sacrificing American Safety, Office of U.S. Senator Hickenlooper (Jan. 12, 2026), https://www.hickenlooper.senate.gov/press_releases/hickenlooper-gallego-colleagues-call-out-trump-admin-for-diverting-federal-agents-for-immigration-enforcement-sacrificing-american-safety/ [<https://perma.cc/G257-PBN2>] (noting that the effects of diverting agents away from their duties to assist with civil immigration enforcement “are especially devastating at HSI – an agency the U.S. relies on to combat child exploitation, dismantle human trafficking networks, stop fentanyl pipelines, and combat cartels and other criminal organizations.”).

⁷⁸ See Department of Homeland Security, *Consolidated Lead Evaluation and Reporting (CLEAR) digital data system*, Contract Award No. GS-02F-026DA, SAM.gov (Mar. 31, 2026), <https://sam.gov/opp/49b555c3a4574efcbf5e8f6025014233/view> [<https://perma.cc/Y64Q-GE3H>] [hereinafter DHS CLEAR Contract].

The CLEAR platform provides law enforcement users with access to information that constitutes “personal data” under Maryland law because it “is linked or can be reasonably linked to an identified or identifiable consumer.” CLEAR synthesizes data from many different sources. According to research by *New York Times* journalist McKenzie Funk published a few years ago, “CLEAR is powered by personal information: data from credit agencies, cellphone registries, social-media posts, property records, utility accounts, fishing licenses, internet chat rooms and bankruptcy filings, all fused and vetted by algorithm to form an ever-evolving, 360-degree view of U.S. residents’ lives.”⁷⁹

A substantial portion of the data integrated into CLEAR does not fall into the “publicly available information” exception to the definition of “personal data,” under which data is not “personal data” if the person in possession of it (in this case Thomson Reuters) “[l]awfully obtains [the information] from a record of a governmental entity, if the person complies with each restriction or term of use that the governmental entity imposes as a condition for providing the information to the person.”⁸⁰ Thomson Reuters touts the product’s “vast collection of public and proprietary records,”⁸¹ indicating that it intermixes information that may fall under the publicly available information exception with other, “proprietary” personal data that does not. For example, cell phone data included in CLEAR almost certainly come from private entities, not government records.⁸² This is how Thomson Reuters described the cell phone data available through CLEAR to the Hagerstown Police Department in 2025:

- Cell Phone Data – CLEAR’s phone data is the most comprehensive, current, and accurate data in the industry. No service other than CLEAR offers gateway access to real-time, nationwide phone data. Through this real-time gateway, CLEAR provides comprehensive phone data, including detailed carrier contact information, for cell phones, landlines, and VoIP. Additionally, the Phone Records data set

⁷⁹ McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, N.Y. Times (Oct. 2, 2019), <https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html> [<https://perma.cc/B752-7AAQ>].

⁸⁰ Commercial Law § 14-4701(cc)(1)(i) (2025); HB 711, *supra* note 14 (modifying this definition).

⁸¹ *Prevent Fraud, Detect Risk, and Investigate Crime with Powerful Online Investigation Software*, Thomson Reuters, <https://legal.thomsonreuters.com/en/products/clear> [<https://perma.cc/35FA-PDQC>].

⁸² See DHS CLEAR Contract, *supra* note 78, at 2.

provides access to hundreds of millions of phone records, including more than 200 million cell phone numbers, as well as landlines and VoIP numbers.⁸³

In addition, it is possible that to the extent Maryland state and local agencies have shared data with Thomson Reuters, they have done so on the agreement that the company not repackage and resell that data. Indeed, Maryland law directs “each governmental entity . . . [to] develop and publish procedures that prevent the sale and redisclosure of personal records and sensitive data provided or made available by the governmental entity in a way that harms the privacy of residents of the State.”⁸⁴ Such procedures are to consider “any possible contractual limitations on the sale or redisclosure of personal records or sensitive data that a governmental entity may place on a person who receives personal records or sensitive data that are provided or made available by the governmental entity,”⁸⁵ to “discourage the development of a secondary commercial market for personal records or sensitive data that are provided or made available by a governmental entity,”⁸⁶ and to “limit a person who receives personal records or sensitive data that are provided or made available by a governmental entity from selling or redisclosing the data with other persons.”⁸⁷ In light of the large volume of government-derived data included in the CLEAR platform, Attorney General Brown should ensure that Thomson Reuters honors restrictions placed on any information obtained from units of Maryland government.

C. LexisNexis impermissibly sells Marylanders’ personal data to immigration enforcement authorities.

Like Thomson Reuters, LexisNexis not only sells Marylanders’ sensitive data in violation of Maryland privacy law, as discussed above, but also violates Maryland law by selling non-sensitive personal data to an agency that engages in civil immigration enforcement as part of the LexisNexis “Accurint” product. According to information

⁸³ Letter from Jon Dubs to Kristy E. Carroll, *supra* note 53; *see also* Letter from Adam Oehmke to Brooke Lindemann, *supra* note 53.

⁸⁴ MD Code, State Government, § 10-1702(b)(1); HB 711, *supra* note 14 (replacing “geolocation” with “sensitive”).

⁸⁵ State Government § 10-1702(b)(2)(i); HB 711, *supra* note 14.

⁸⁶ State Government § 10-1702(b)(2)(iii)(2); HB 711, *supra* note 14.

⁸⁷ State Government § 10-1702(b)(2)(iii)(3); HB 711, *supra* note 14.

uncovered by researchers at Just Futures Law using Freedom of Information Act requests,⁸⁸ ICE has made heavy use of this service in Maryland.⁸⁹ According to one summary that the researchers obtained of ICE's use of LexisNexis's Accurint service, between February and September 2021, the Baltimore field office of ICE Enforcement and Removal Operations made 2,193 searches using the platform and generated 352 reports.⁹⁰

Accurint "helps law enforcement swiftly identify individuals, their assets, addresses, phones, relatives, and associates. The powerful search capabilities enable quick compilation of . . . records, from thousands of sources, that would take days to collect individually."⁹¹ Accurint provides law enforcement users with "access to 10,000 public records and state & local RMS and CAD data from over 1,500 agencies nationwide, all in one search."⁹² Source data includes:

- Incarceration data,
- Court records,
- DMV records,
- Property ownership records,
- Liens, judgments, and UCC records,
- Marriage and birth records, and
- Business records.⁹³

⁸⁸ *JFL v. ICE (Data Broker FOIA)*, Just Futures Law, <https://www.justfutureslaw.org/jfldatabrokerfoia> [<https://perma.cc/T2UQ-KPUU>].

⁸⁹ *DHS-ICE AVCC Usage September 2021* (Sept. 2021) (accessible at page 2 of the following document), <https://www.justfutureslaw.org/s/ICE-ERO-Accurint-Summary-Data-and-Data-Subscription-Services-InfoDec2021.pdf> [<https://perma.cc/C6HE-WWZ8>].

⁹⁰ *Id.* at 5.

⁹¹ *Accurint for Law Enforcement*, LexisNexis Risk Solutions, <https://risk.lexisnexis.com/products/accurint-for-law-enforcement> [<https://perma.cc/8CEU-EW4N>].

⁹² Email from LexisNexis Special Sales Executive, *Subject: Welcome to Accurint Virtual Crime Center (Part 1: ID for Sign-in)* (Feb. 2021) (accessible at page 14 of the following document), <https://www.justfutureslaw.org/s/ICE-ERO-Accurint-Summary-Data-and-Data-Subscription-Services-InfoDec2021.pdf> [<https://perma.cc/C6HE-WWZ8>].

⁹³ Hannah Lucal et al., *How Data Brokers Assist ICE in Cook County*, Mijente, Just Futures Law at 3, <https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/65283e83622fff1ee8837590/1697136260425/Final+Cook+County+Fact+Sheet+and+Graphic+2.pdf> [<https://perma.cc/A56J-3X2H>].

A key feature of Accurint is that it provides information not only about a target individual, but also about that individual's relatives, neighbors, and associates.⁹⁴

III. Companies violate Maryland privacy law by selling Marylanders' motor vehicle records to immigration enforcement authorities in circumstances not required by the federal Driver's Privacy Protection Act.

Multiple companies also violate Maryland privacy law because they sell Marylanders' motor vehicle records to immigration enforcement authorities in ways that are permitted, but not required, by the federal Driver's Privacy Protection Act (DPPA) – and that thus are no longer exempt from Maryland privacy law. Again, under Maryland law, a data controller may not “knowingly sell the personal data of a consumer to a federal, State, or local governmental unit that, within the 6 months that immediately precede the sale of the personal data, has engaged in or supported civil immigration enforcement through the provision of personnel or material resources,”⁹⁵ and “personal data” is “any information that is linked or can be reasonably linked to an identified or identifiable consumer.”⁹⁶ Although there has long been a limited exception to Maryland privacy law for certain activities permitted under the DPPA, under applicable Maryland law as modified by HB 711 effective July 1, this exception now only extends to data “collected, processed, sold, or disclosed *as required by* the federal Driver's Privacy Protection Act of 1994.”⁹⁷ Under the federal Driver's Privacy Protection Act (DPPA), personal information in connection with a motor vehicle record “shall be disclosed” – or in other words is required to be disclosed – for limited purposes, including matters of:

- motor vehicle or driver safety and theft;
- motor vehicle emissions;
- motor vehicle product alterations, recalls, or advisories;

⁹⁴ Joseph Cox, *LexisNexis 'Virtual Crime Center' Makes Millions Selling to the Government*, Vice (Feb. 2, 2023), <https://www.vice.com/en/article/lexisnexis-selling-data-government/> [<https://perma.cc/2MBE-RX4N>].

⁹⁵ HB 711, *supra* note 14 at p. 6 ¶¶ 4–8 (Md. 2026) (revising Commercial Law § 14–4707(a)).

⁹⁶ Commercial Law § 14–4701(w)(1).

⁹⁷ Commercial Law § 14–4703(b)(8); HB 711, *supra* note 14 (replacing “in compliance with” with “as required by”).

- performance monitoring of motor vehicles and dealers by motor vehicle manufacturers; and
- removal of non-owner records from the original owner records of motor vehicle manufacturers.⁹⁸

The DPPA also sets forth a large number of circumstances in which personal information in connection with a motor vehicle record “may be disclosed” — or in other words is permitted, but *not required*, by the DPPA.⁹⁹ In circumstances that only fall into the permissible categories, there is no longer an applicable exception under Maryland privacy law, and thus any commercial processing or use of those records are only permissible to the extent otherwise allowed under Maryland privacy law.¹⁰⁰

A. Thomson Reuters impermissibly sells Marylanders’ motor vehicle records to immigration enforcement authorities.

Thomson Reuters violates Maryland privacy law by selling Marylanders’ motor vehicle records to the Department of Homeland Security because motor vehicle records are included in the Thomson Reuters CLEAR product that it provides to the Department of Homeland Security.¹⁰¹ According to public-facing web resources provided by Thomson Reuters, “the platform generally offers access to core identity and vital statistics, including names, government-issued identifiers, driver’s-license details,” and many other types of information.¹⁰² Driver’s license details include driver’s license numbers.¹⁰³ CLEAR documents from 2025 state that “CLEAR offers real-time gateway access to vehicle registration data for 43 states, the District of Columbia,

⁹⁸ 18 U.S.C. § 2721(b).

⁹⁹ 18 U.S.C. § 2721(b)(1)–(14).

¹⁰⁰ Commercial Law § 14–4703(b)(8); HB 711, *supra* note 14 (replacing “in compliance with” with “as required by”).

¹⁰¹ See DHS CLEAR Contract, *supra* note 78.

¹⁰² *Public Records Privacy Statement*, Thomson Reuters, <https://legal.thomsonreuters.com/en/legal-notices/privacy-records> [<https://perma.cc/9Z92-END4>] (last updated Jul. 11, 2025).

¹⁰³ See State of Michigan Procurement, Notice of Contract No. 200000000689 (Apr. 1, 2020), <https://cdt.org/wp-content/uploads/2021/12/Notice-of-Contract-No-200000000689-State-of-Michigan-1-8-million-West-Publishing-Corporation-2020-2023.pdf> [<https://perma.cc/UA6Y-Y6BL>] (stating that contractor must be able to provide driver’s license number). *CLEAR Skip Tracing Features*, Thomson Reuters, <https://legal.thomsonreuters.com/en/products/clear-skip-tracing/features> [<https://perma.cc/5ZVK-QCCA>] (explaining that searches on specific data elements enable users to “[f]ind information like addresses, business names, driver’s license numbers, and email addresses”).

and Puerto Rico, providing up-to-date information on vehicles and their registered owners.”¹⁰⁴

As of the drafting of this Consumer Complaint, the additional terms and disclaimers provided by Thomson Reuters regarding proper use of specific data sources available through CLEAR note the particular state laws that apply to use of driver’s license data related to Florida and Texas, but contain nothing specific about Maryland driver’s license data.¹⁰⁵ In addition, the “disclaimer and legal terms” that apply to general driver license data suggests that CLEAR users likely can access this data after attesting to a use that is merely “permissible,” but not required,” under the DPPA.¹⁰⁶

B. LexisNexis impermissibly sells Marylanders’ motor vehicle records to immigration enforcement authorities.

LexisNexis also violates Maryland privacy law by selling Marylanders’ motor vehicle records, which are part of the LexisNexis Accurint product, to the Department of Homeland Security.¹⁰⁷ For example, a report generated in Accurint includes the target person’s driver’s license(s) state(s) and number(s).¹⁰⁸

Similar to the CLEAR platform, the Accurint platform likely only forces users to certify a use that is “permissible,” but not required, under the DPPA.¹⁰⁹

REQUEST FOR RELIEF

The privacy rights that this Request calls on Attorney General Brown to vindicate are needed to ensure the safety and wellbeing of Marylanders. When Marylanders’ privacy rights are not protected, they suffer harm.

¹⁰⁴ Letter from Jon Dubs to Kristy E. Carroll, *supra* note 53; *see also* Letter from Adam Oehmke to Brooke Lindemann, *supra* note 53.

¹⁰⁵ *CLEAR and Westlaw Public Records (Risk & Fraud) Supplier Additional Terms & Disclaimers*, Thomson Reuters (May 14, 2026), <https://www.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/other/clear-additional-terms.pdf> [<https://perma.cc/4WJ6-C5P6>].

¹⁰⁶ *Id.* (“Your use of this data may be subject to privacy restrictions imposed by Driver’s Privacy Protection Act (‘DPPA’) and state law. If you access motor vehicle, driver’s license, state boat, or similar data, you will be required to acknowledge compliance with the law and to choose among ‘permissible uses’ for the data.”).

¹⁰⁷ *See* DHS CLEAR Contract, *supra* note 78.

¹⁰⁸ *See* LexisNexis Risk Solutions, *Accurint Virtual Crime Center Get Started*, YouTube (Oct. 17, 2025), <https://www.youtube.com/watch?v=FZLKKETsBy8&t=3m46s>, [<https://perma.cc/XVS8-M8TA>].

¹⁰⁹ *See* LexisNexis Master Terms & Conditions – Government (Feb. 2023), <https://risk.lexisnexis.com/masterterms/government> [<https://perma.cc/FC4D-JT8Q>].

Moreover, Marylanders have made clear that they want more privacy safeguards. Indeed, Marylanders clamored for legislative protections for their privacy as embodied by the Maryland Driver Privacy Act in 2021, the Maryland Online Data Privacy Act in 2024, the Maryland Values Act in 2025, and the Maryland Data Privacy Act in 2026. Each of these legislative measures passed with overwhelming support from Marylanders' elected representatives. Marylanders also speak up in defense of their privacy. For example, when the Baltimore Board of Estimates recently considered and approved the Baltimore Police Department's purchase of vehicle location data from Thomson Reuters, residents reportedly were outraged.¹¹⁰ In the words of one resident, "There's a big difference between being seen in public and then someone being able to pull up records to know where you were every moment in public over the last 10 years."¹¹¹

Initiating investigations and enforcement actions regarding the numerous legal violations described in this Request would also be consistent with Attorney General Brown's goals. The recent letter to Congress from Attorney General Brown and 16 other state AGs called for all of the following:

- Prohibit the federal government from purchasing sensitive personal data, geolocation information (including that associated with mobile advertising IDs (AdIDs or MAIDs) or vehicles), or web browsing history of Americans from data brokers;
- Require federal law enforcement to obtain judicial warrants before acquiring and/or searching Americans' web browsing data, search queries, and location information, as well as before using AI to identify data subjects;
- Reasonably regulate private data brokers to improve transparency over their data collection, maintenance, analysis, sale, and disclosure practices, and to give consumers greater control over the data collected and sold about them. Such regulations should not preempt more robust state laws and regulations applicable to the collection, sharing, and sale of personal information.

¹¹⁰ Fern Shen, *License Plate Reader Technology for Baltimore Police Approved Despite Public Opposition*, Baltimore Brew (Mar. 5, 2026), <https://www.baltimorebrew.com/2026/03/05/license-plate-reader-technology-for-baltimore-police-approved-despite-public-opposition/> [<https://perma.cc/XQJ3-2KNL>].

¹¹¹ *Id.*

All of these goals can be accomplished under existing Maryland law, and we urge Attorney General Brown to use his full authority to achieve them.

CONCLUSION

The data industry harms Marylanders and violates Maryland's strong privacy laws. Attorney General Brown should take immediate action to rein in the harmful practices detailed in this Request. Specifically, we call on Attorney General Brown to investigate and initiate enforcement against the companies named in this Request for the violations detailed above. We look forward to continuing to work with and support the Attorney General and the staff of his office in this important effort.

By:

/s/

Laura M. Moy
Technology Law Clinic
at Georgetown Law
600 New Jersey Ave NW
Washington, DC 20001

Counsel for We Are CASA

August 19, 2026

Respectfully submitted,

We Are CASA
Center for Democracy & Technology
Center on Privacy & Technology at
Georgetown Law
Consumer Federation of America
Council on American-Islamic
Relations
Demand Progress Education Fund
Electronic Frontier Foundation
Electronic Privacy Information
Center
Fight for the Future
Surveillance Technology Oversight
Project