Statement of

Laura Moy, Associate Professor of Law, Georgetown University Law Center

before the Senate Finance Committee

Hearing on SB 504, Data Privacy – Consumer Data,
Public Records, and Message Switching System (Data Privacy Act)

February 26, 2026

Good afternoon, Chair Valderrama, Vice Chair Charkoudian, and distinguished members of the Committee. Thank you for permitting me to share testimony on this important topic today. I am Laura Moy, an associate professor of law at Georgetown University, and a scholar of surveillance and privacy law.[1] I also direct the Communications & Technology Law Clinic at Georgetown, in which capacity I represent nonprofit clients on various matters at the intersection of law and technology. Among my clients is CASA, which I have been supporting on issues related to privacy legislation. In addition, I am a proud Marylander. I grew up in the state and have lived there for almost my entire life.

Over 20 years ago, when I graduated from the University of Maryland, I moved to New York and I went to work for the Manhattan DA's office. During the years I spent there between college and law school, I used a lot of data. I served as an investigative analyst, helping to locate and investigate people using state records and also private data broker services. I learned how to process cell site location information—the same type of cell phone location records at issue in the *Carpenter* case decided in the Supreme Court a few years ago[2]—and by the end of my time there, I was a full-time location data analyst in the Computer Forensics Unit.[3]

And then I went to law school and I became a privacy lawyer, and it is in that capacity, with that context, that I appear before you today.

This is all to say that I understand the power of data well, and I understand how data from disparate sources can be pieced together to construct a detailed picture of

[1] My full CV, including links to my scholarly writings and past legislative testimony, can be found at https://lauramoy.com/.
[2] *See* Carpenter v. United States, 585 U.S. 296 (2018).
[3] *See* Laura Moy, *I Used to Track Cell Phone Location Information for Prosecutors*, Hacker Noon (Nov. 28, 2017), https://hackernoon.com/i-used-to-track-cell-phone-location-information-for-prosecutors-b0dbd4325997 [https://perma.cc/BP2Q-V53T].

someone's life. In fact, I think and worry about this a lot. I think about it when I order a prescription online. I think about it when I use a navigation app to try to figure out which route to my office in DC will be the least congested with rush hour traffic. I think about it when I pull up to the gate at a parking garage and, before I even reach out to push the button for a ticket, the gate lifts and the screen shows that my license plate number has been recorded. I think about it when my kid's school asks me to sign a consent form for apps and services that teachers may wish to use to support their teaching.

And, of course, I also think deeply about the power of data when I read story after story about ICE agents descending on Maryland homes and businesses to take people from their families and communities and send them hundreds or even thousands of miles away.

ICE has powerful surveillance capabilities fueled by for-profit data brokers.

In the first nine months of the second Trump administration, ICE detained some 3,300 Marylanders.[4] This was done with the assistance of a vast surveillance network powered by private companies. Some highlights of ICE's astonishing surveillance capabilities:

- An ICE agent can search for the license plate of that person's car and receive a list of times and places where it has recently been spotted by cameras, as well as predictions about where it is likely to be seen in the future.[5] This tool can also be configured to send an agent a push notification when the vehicle is next seen.[6]
- ICE agents can also track a person's phone over time and even follow it from home to work.[7] They can even search for all of the phones in a particular neighborhood, then view the locations where all of those phones go when they leave the neighborhood to go to work or church.[8]

---

[4] Nicole Pilsbury, *More than 3,300 Marylanders Were Detained by ICE in 2025, Twice the Number of Preceding Years*, Maryland Matters (Jan. 11, 2026), https://marylandmatters.org/2026/01/11/more-than-3300-marylanders-were-detained-by-ice-in-2025-twice-the-number-of-preceding-years/ [https://archive.ph/O5bLN].

[5] Joseph Cox, *This App Lets ICE Track Vehicles and Owners Across the Country*, 404 Media (Nov. 17, 2025), https://www.404media.co/this-app-lets-ice-track-vehicles-and-owners-across-the-country/ [https://archive.ph/LGkVd].

[6] *Id.*

[7] 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].

[8] *Id.*

- An ICE agent can take a picture of a person's face and then try to identify them in real time using facial recognition.[9] This tool has been known to make errors.[10]

The companies that provide ICE with these surveillance tools use troves of data to power their services. Among the data sources that fuel these surveillance capabilities are:

- A vast nationwide network of cameras, including speed cameras, security cameras, parking garage cameras, and cameras mounted on certain vehicles;[11]
- Location data brokers, which receive location data about individual people's devices from a variety of sources, including ad networks, typically without people's awareness;[12]
- State and local government records, such as records about people's driver's licenses and vehicle registrations;[13] and

[9] Joseph Cox, *You Can't Refuse To Be Scanned by ICE's Facial Recognition App, DHS Document Says*, 404 Media (Oct. 31, 2025), https://www.404media.co/you-cant-refuse-to-be-scanned-by-ices-facial-recognition-app-dhs-document-says/ [https://archive.ph/Br5MT].

[10] *See* Joseph Cox, *ICE's Facial Recognition App Misidentified a Woman. Twice*, 404 Media (Jan. 19, 2026), https://www.404media.co/ices-facial-recognition-app-misidentified-a-woman-twice/ [https://archive.ph/oONPC].

[11] *See Records Reveal ICE Using Mass Surveillance Database to Track People With Aid of Local Law Enforcement*, ACLU (Mar. 13, 2019), https://www.aclu.org/press-releases/records-reveal-ice-using-mass-surveillance-database-track-people-aid-local-law (explaining that "Vigilant Solutions' database allows the agency to pinpoint the locations of drivers going about their daily private lives, and gives it access to over 5 billion points of location information collected by private businesses like insurance companies and parking lots."); Joseph Cox, *This App Lets ICE Track Vehicles and Owners Across the Country*, 404 Media (Nov. 17, 2025), https://www.404media.co/this-app-lets-ice-track-vehicles-and-owners-across-the-country/ [https://archive.ph/LGkVd].

[12] *See* 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].

[13] *See* DHS-ICE LexisNexis Accurint Summary of Data and Data Subscription Services obtained by Just Futures Law (Dec. 2021), https://www.justfutureslaw.org/s/ICE-ERO-Accurint-Summary-Data-and-Data-Subscription-Services-InfoDec2021.pdf, at 12 (explaining that the LexisNexis Accurint database in use by ICE "provides access to public records and state and local record management systems (RMS) and computer-aided dispatch (CAD) data from over 1,500 agencies nationwide, all in one search."). In addition to the records that data brokers claim to offer, it recently came to light that Maryland has been permitting ICE unfettered access to MVA records on an automated and instantaneous basis—despite the 2021 passage of the Maryland Driver Privacy Act prohibiting this. *See Wyden, Espaillat and 38 Members of Congress Urge Democratic Governors to Block ICE from Accessing Americans' DMV Data* (Nov. 12, 2025), https://www.wyden.senate.gov/news/press-releases/wyden-espaillat-and-38-members-of-congress-urge-democratic-governors-to-block-ice-from-accessing-americans-dmv-data.

- Federal records, such as tax and Medicaid records improperly shared with ICE.[14]

To rein in the improper collection, aggregation, and abuse of Marylanders' data, we must act now to pass the Maryland Data Privacy Act. It is particularly important to strengthen legal protections for location information about people and vehicles, and close loopholes that data brokers may be exploiting to share sensitive private information with law enforcement.

The Maryland Data Privacy Act is needed to rein in the for-profit surveillance industry.

Fortunately for all of us sitting in this room, five years ago, with the support and leadership of many people in this room, Maryland passed the Maryland Driver Privacy Act. And two years ago, Maryland passed the Maryland Online Data Privacy Act, MODPA, which went into effect last October. These are strong state privacy laws working to safeguard both the information that the government holds about us and the data that private companies collect about us. And yet, in this moment, we are constantly being reminded of some of the ways in which these protections could be even stronger and clearer, and could better protect our friends, neighbors, and families from the data brokers and surveillance companies that ICE relies on. I'm here to talk about a few of those recommendations today.

1. **This bill would ensure that MODPA more clearly protects against the sale of vehicle location data.** Maryland's commercial privacy law applies heightened protection to a person's precise location.[15] And as we all know, most of the time—including when I am at home, at work, waiting to pick my child up from sports practice, or on the road between here and Bethesda—the location of my car is functionally equivalent to the location of me.[16] MODPA could be clearer

[14] *See* Fatima Hussein, *Data of Thousands of Taxpayers Wrongly Shared with DHS, Court Filing Says,* PBS News, (Feb. 12, 2026) https://www.pbs.org/newshour/politics/data-of-thousands-of-taxpayers-wrongly-shared-with-dhs-court-filing-says [https://archive.ph/CvnXZ].
[15] Md. Code Ann., Com. Law § 14-4701(gg) (defining "sensitive data," which cannot be sold, to include "precise geolocation data").
[16] *See* United States v. Jones, 565 U.S. 400 (2012).

about this.[17] As explained above, we know that this information is being collected and sold for profit,[18] including to ICE.[19] That information should not be for sale.

2. **This bill would narrow MODPA's carve-out for "publicly available information."** Maryland's commercial privacy law generally does not apply to "publicly available information," which makes sense. But the definition of what constitutes "publicly available" is overbroad.[20] Types of information that we consider sensitive, such as location data or data about a person's religious beliefs or citizenship status, should never be considered "publicly available." Even when we share this information with another party or allow the government to hold it, we still think of it as private. Maryland's privacy law should be refined to clarify that sensitive information never falls within the "publicly available information" carve-out—it must always be protected.

3. **This bill would also narrow MODPA's carve-out for sharing of information with law enforcement.** As currently written, MODPA explicitly does not restrict a data controller or processor's ability to comply with a "civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, State, local, or other governmental authority."[21] This is far too broad. When private companies, including data brokers, sell or share information with law enforcement, this enables law enforcement to make an end-run around the

[17] Md. Code Ann., Com. Law § 14-4701(x)(1) (defining "precise geolocation data" as "information derived from technology that can precisely and accurately identify the specific location of a *consumer*, within a radius of 1,750 feet") (emphasis added).
[18] *See Law Enforcement and Technology: Use of Automated License Plate Readers*, CRS Report No. R48160 (Aug. 19, 2024), https://www.congress.gov/crs_external_products/R/PDF/R48160/R48160.3.pdf; Jay Stanley, *Flock's Aggressive Expansions Go Far Beyond Simple Driver Surveillance*, ACLU (Sep. 18, 2025), https://www.aclu.org/news/privacy-technology/flock-roundup.
[19] Cooper Quintin, *ICE Is Going on a Surveillance Shopping Spree*, EFF (Jan. 7, 2026), https://www.eff.org/deeplinks/2026/01/ice-going-surveillance-shopping-spree; Joseph Cox, *This App Lets ICE Track Vehicles and Owners Across the Country*, 404 Media (Nov. 17, 2025), https://www.404media.co/this-app-lets-ice-track-vehicles-and-owners-across-the-country/ [https://archive.ph/LGkVd].
[20] Md. Code Ann., Com. Law § 14-4701(cc) (defining "publicly available information" generally to include information that a person "[l]awfully obtains from a record of a governmental entity," "reasonably believes a consumer or widely distributed media have lawfully made available to the general public," or "obtains from a person to whom the consumer disclosed the information"). For discussion of consumer complaints in another state regarding misuse of "publicly available" information, *see* Connecticut Office of the Attorney General, *CTDPA Enforcement Report 2025*, https://portal.ct.gov/-/media/ag/press_releases/2026/annual-report-final-2.pdf, at 2 (noting that a large portion of consumer complaints received "involved people search websites that purportedly combine 'publicly available' records" and that the profiles created based on these records "are a far cry from public information and should not be carved out from the reach of privacy enforcers," and recommending legislative narrowing of "publicly available information" under Connecticut law to ensure coverage over data brokers).
[21] Md. Code Ann., Com. Law § 14-4701(a)(2).

Fourth Amendment.[22] We're seeing this right now with ICE, buying access to troves of data that ICE then uses to build a detailed picture of Marylanders' lives and target individuals and communities for deportation. To help stem the flow, the law enforcement exception should be modified to establish a warrant standard in situations involving immigration enforcement.

4. **This bill also offers a series of minor revisions to the Maryland Public Information Act and Public Safety Article to clarify existing obligations of Maryland state and local government entities under the Maryland Driver Privacy Act.** Under that law, units of state and local government are required to deny access to records to those seeking access for the purpose of immigration enforcement unless presented with a valid judicial warrant.[23] This bill would add additional minor provisions to clarify that custodians of records must include this in their regulations and procedures, and must make some effort to find out whether seekers of records seek them for immigration enforcement purposes so that they know whether or not a warrant standard applies.

5. **Finally, this bill would also provide clarification regarding the important work state and local government entities are currently doing in coordination with the Department of IT, developing procedures to prevent the sale and redisclosure of public records.**[24] The bill would clarify that this work should include a particular emphasis on sensitive information, such as health data, citizenship status, and information about children.

Thank you for permitting me to testify in support of this important bill. I look forward to your questions.

---

[22] *See* Anika Venkaesh & Lauren Yu, *DHS Is Circumventing Constitution by Buying Data It Would Normally Need a Warrant to Access*, ACLU (Jan. 12, 2026), https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access.

[23] Md. Code Ann., Gen. Provis. § 4-320.1.

[24] Maryland HB 1222 (2025) (adding Md. Code Ann., St. Govt. §10-1702, directing governmental entities, in coordination with the Department of Information Technology, to develop and publish procedures preventing the sale and redisclosure of personal records and geolocation data shared with outside parties).