AI Surveillance: Need for Regulatory Safeguards

I. Purpose and Overview

The U.S. government's use of Artificial Intelligence (AI) surveillance has increased rapidly in the last five years. For example, the Federal Bureau of Investigations (FBI) has access to over 640 million photographs that can be used for facial recognition. In 2025, Congress passed the Big Beautiful Bill, which made ICE the highest-funded law enforcement agency in the country. ICE is using those funds to acquire powerful surveillance tools in furtherance of the Trump administration's mass detention and deportation agenda, including fingerprinting and performing facial recognition on citizens and immigrants in real time, monitoring social media, and searching license plate data.

Private companies develop AI that maximizes their profits without regulation. The lack of a comprehensive federal data privacy law allows private companies to collect personal information without limitation, transfer that data to law enforcement and other private companies, and make inferences and predictions about individuals with few safeguards for rights, security, bias, and transparency. Legal practitioners warn that the development of AI with unfettered access to personal information and increased use of this technology by federal and state law enforcement for surveillance poses serious risks to privacy, safety, civil liberties, and civil rights, and perpetuates and furthers bias and discrimination.

While AI systems may offer efficiency and other positive applications for federal and state governments, and the data obtained through AI surveillance may aid public safety, the use of AI surveillance should occur only with public understanding and feedback, notice and informed consent, and authorization by all relevant legislative bodies. President Trump and his loyalists are eroding due process and the rule of law, and the continued use of AI surveillance without regulation will further erode the rights of people living in the United States, including First and Fourth Amendment rights.

This Memo sets forth the principles that should govern AI surveillance of people living in the United States regardless of citizenship status. The Memo begins with a brief description of AI, ethical concerns, and current U.S. regulation of AI. The Memo then discusses various types of surveillance technology, including AI powered surveillance. The Memo concludes with a suggested regulatory framework for AI surveillance and a call for comprehensive privacy legislation in the United States.

II. Background

A. AI Generally

Artificial Intelligence has many definitions. AI is technology that integrates models and algorithms enabling machines/computers to simulate human learning and perform tasks such as problem-solving and decision-making. An algorithm is a set of instructions for solving a problem. An AI model is a program that has been trained on a set of data to recognize certain patterns or make certain decisions, applying different algorithms to data inputs to achieve tasks (or outputs).

AI models are trained on vast amounts of data. AI models search for patterns in this data and make predictions and inferences based on this data. AI developers aggregate (and often scrape) data from both public and private sources, including websites, social media, apps, and consumer transactions. AI developers also purchase data from commercial data brokers that obtain data through the government, apps, public records, insurance companies, etc., without the knowledge or permission of the owners of that personal data. There is little transparency regarding how AI models work and the origin of the training data.

B. AI Ethical Concerns

AI can create opportunities, such as facilitating medical diagnoses, automating repetitive tasks and assessing financial and cybersecurity threats, but there are ethical concerns and risks in using AI and relying on the outputs. Section III of this Memo discusses use of AI for surveillance and related legal concerns.

Transparency, bias, discrimination and disparate impact are all ethical challenges of using AI. Historically, communities of color have been disproportionately affected by law enforcement including surveillance, stops and arrests, and using AI can exacerbate bias and discrimination.

There are ethical concerns at all stages of the AI life cycle. AI models often use inaccurate, insufficient, incomplete, biased, and flawed data to train AI applications/models. Outputs lack emotional intelligence, empathy, morality, and ethics. Using data regarding a specific group to train a model or as an input / prompt may lead to opportunities only for certain groups and loss of freedoms and punishments for other groups. AI can reinforce societal biases, subordination of groups, discrimination, underrepresentation, and denigration of human dignity.

There are other ethical concerns with AI generally, including impact on the environment, employment, education, and media, potential job loss, deepfakes, weapons automation, social manipulation, etc., none of which will be discussed in this Memo.

C. Current U.S. Government AI Regulations

Innovation is outpacing regulation of AI. The U.S. has not enacted a comprehensive AI Act nor a comprehensive privacy law.

The 2020 AI in Government Act created a center to facilitate government AI adoption and instructed the Office of Management and Budget (OMB) to issue guidance regarding government AI adoption and policy development. OMB was asked to set out best practices to mitigate AI's discriminatory impact.

In December 2022, Congress passed the Advancing American AI Act, which defines principles for government use of AI and requires an inventory of agency AI and the development of further guidance from OMB. The Department of Homeland Security (DHS) was directed to issue policies and procedures that would give "full consideration to the privacy, civil rights, and civil liberties impacts of artificial intelligence-enabled systems."

In October 2023, President Joe Biden issued Executive Order 14110 requiring federal agencies to take additional steps to protect Americans' privacy, civil liberties, and civil rights, including by improving "the collection, reporting, and publication of agency AI use cases."

In March 2024, OMB issued a memorandum requiring agencies to institute a risk assessment framework for their AI systems beginning in December 2024. Agencies were required to report their AI systems that affect people's rights or safety, explain the risks of the AI systems, and cease use of any AI system the agencies could not bring into compliance with the OMB's framework. A second OMB Memo released in September 2024 included best practices and specific requirements for managing AI risks and performance and managing business processes in acquiring AI.

While the Biden OMB Memos suggest that the federal government recognized privacy and civil liberties concerns in using AI, there are exceptions for national security, domestic intelligence, and law enforcement; and federal agencies can request an opt-out for reporting on the use of and risks of using an AI system due to undue hardship on the agency.

President Trump rescinded Biden's October 2023 AI Executive Order upon taking office in 2025 and signed Executive Order 14179 "Removing Barriers to American Leadership in Artificial Intelligence." The Biden OMB Memos have been rescinded and replaced by two Memos that provide AI guidance for federal agencies. These Trump administration OMB Memos encourage accelerated adoption of AI by reducing bureaucratic burdens and restrictions and by allowing waivers for AI use cases and transparency requirements when justified. The Trump OMB Memos do not require the minimum risk management practices for "rights-impacting" and "safety-impacting" AI that were set forth in the Biden OMB Memos.

D. Summary of Department of Homeland Security and Department of Justice AI Usage

The use of AI by DHS for both surveillance and other purposes has increased from 2024 to 2025. Uses include facial recognition, license plate capture, location tracking, fingerprinting, validating identity, sentiment analysis, and crime prediction. In 2024, DHS used a total of 197 AI technologies. The FY2025 DHS Budget included "additional AI funds" for both ICE and CBP. Per the 2025 DHS AI Use Case Inventory, DHS is using a total of 235 AI technologies (CBP is using 83 and ICE 51). In a 2024 deep dive into its AI use cases, DHS identified 39 safety and/or rights impacting use cases, with 14 of the deployed AI use cases involving face recognition and face capture technologies. In 2025, there were 55 high impact and 60 "presumed high-impact, but determined not high-impact" use cases.

The 2025 Department of Justice AI Use Case Inventory includes 315 entries, a 30.7% increase from the 2024 inventory.

III. AI Surveillance Technology, Legal Concerns, and Proposed Solutions

State and federal agencies have been purchasing significant amounts of personal data and commercially available information (CAI), some of which is highly sensitive (hereinafter, collectively "personal data"), from commercial data brokers without regulation and transparency. CAI includes biometric data, health data, location data, and financial data. Highly sensitive CAI includes information "not widely known

about an individual that could be used to cause harm to the person's reputation, emotional well-being or physical safety"

Public safety, verifying citizenship and immigration status, and issuing identification are all governmental responsibilities. In order to fulfill these responsibilities, it is reasonable that federal and state governments will need to collect and retain some personal data about individuals in and coming into the United States. However, the current approach seems to embody a "collect it all" approach that emerged from the post 9/11 surveillance state.

AI technology automates usage and analysis of personal data. With a few clicks, the government can access our intimate information, including information concerning healthcare, political action, associates, identities, and beliefs. As noted above, there are legitimate reasons for law enforcement to use personal data, and it is likely not possible to prohibit such use in totality. However, no one should have to choose between privacy and safety (digital and physical). Regulating how AI is used and personal data is procured and used by state and federal governments can help to protect constitutional rights, civil liberties, and the privacy rights of citizens and immigrants and address concerns of bias, lack of transparency, fairness, and accountability.

Below are some of the commonly used AI surveillance technologies; the list below is not intended to be comprehensive.

A. Surveillance Technologies

1. Facial Recognition and Face Capture

Law enforcement is using both face recognition and face capture technologies. In face capture, a picture of an individual's face is taken and verified and then used in a face recognition system. Face recognition compares an individual's facial features to available images. In 2016, the Georgetown Center on Privacy Technology found that half of all people living in the U.S. are in a law enforcement face recognition database.

A 2020 U.S. Government Accountability Office (GAO) report revealed that approximately 24 million photos had been scraped from websites without first obtaining consent from the one million individuals appearing in those photos. A 2023 GAO report found that several federal law enforcement agencies initially used facial recognition technology without training, and that, as of April 2023, only two agencies required employee training. In its report, the GAO noted that six of the agencies conducted 60,000 searches without training.

The FBI maintains a database with over 640 million images of people residing in the U.S. (2019 statistic). Many of the images were compiled from drivers' license photos from twenty-one states, including states without laws expliciting permitting the use of their driver's license data by third parties. State drivers license photos have been used by ICE as part of its immigration enforcement efforts. At least three states have scanned millions of driver's license photos for ICE. ICE also searched Rhode Island's facial recognition database to find "criminal aliens" using technology provided by L-1 Identity Solutions.

DHS uses both face recognition and face capture AI and in 2024 listed fourteen facial recognition and face capture AI use cases on its website. DHS summarizes face recognition and capture into two categories: automating identity verification during travel, and supporting law enforcement.

CBP issued an RFI in April 2025 requesting information for real-time facial recognition technology that can capture facial images of vehicle occupants at an inbound vehicle point of entry. CBP is already using a biometric matching technology for air, sea, and on land pedestrian entries called Traveler Verification Service, which compares point of encounter photos with travel documents images.

Clearview AI is one of a number of private companies providing facial recognition to state and federal law enforcement. Clearview AI has the largest database with 60+ billion facial images scraped from public websites, mugshot websites, social media, CCTV surveillance cameras, and other open sources. Law enforcement can upload photos of individuals captured via security camera or body-worn camera to Clearview's platform, and the platform tries to match the uploaded faces to images in its platform.

Many of the facial images captured by Clearview AI were scraped without consent from the website owners or the individuals appearing in those images. A class action lawsuit was brought against Clearview AI for violating the Illinois Biometric Information Privacy Act due to its sale of personal images to law enforcement without authorization from the individuals appearing in the photos or the owners of the photos. See *In re Clearview AI, Inc. Consumer Privacy Litigation*, No. 1:21-cv-00135.

ICE has been using Mobile Fortify, a smartphone app created by the Japanese company NEC XXX, that allows ICE officers to scan fingerprints and perform facial recognition on citizens and immigrants since June 2025. The app searches a number of federal databases in real-time for biographical information and immigration status. In a January 2026 lawsuit filed by the State of Illinois and City of Chicago against DHS and the Trump Administration, the Plaintiffs allege that DHS used Mobile Fortify over 100,000 times nationwide on both citizens and non-citizens without consent or the opportunity for individuals to decline use. The State of Illinois and the City of Chicago also allege that DHS has not identified any governance practices for use of Mobile Fortify and that DHS can retain all biometric information collected for fifteen years.

State law enforcement uses ODIN Intelligence's facial recognition system called Homeless Management Information System to identify houseless people who cannot communicate or do not possess identification. Additional personal information is accessible in the system, including date of birth, contact information for family members, probation offices, and therapists, known associates, presence of needles, and arrest history. According to Vice, ODIN Intelligence markets its products as a solution to problems such as "degradation of a city's culture," "reduction of property values," and "poor hygiene."

There have been at least eight wrongful arrests due to erroneous matches by facial recognition programs in the U.S. An African American man spent ten days in jail and his case was not dropped for approximately one year. In seven of these wrongful arrests, law enforcement failed to conduct any investigation, relying solely on the facial match. In 2025, ICE wrongly arrested two U.S. citizens for being "unauthorized aliens."

With 60+ billion facial images accessible to law enforcement and law enforcement's increasing reliance on facial recognition technology instead of traditional investigation techniques, it is probable that wrongful identification will continue. Researchers have found that images of women with darker skin have misclassification rates of up to 34.7% in comparison to error rates of men with lighter skin (error 0-.8%). The National Institute of Standards and Technology (NIST) studied 189 commercial facial recognition programs and found higher rates of false positives for Asian and African American faces compared to Caucasians; these groups were up to 100 times more likely to be misidentified. Biased facial recognition technology will continue to exacerbate racial discrimination.

There are a number of legal concerns with using facial recognition technology. Real-time biometric surveillance could chill First Amendment rights of free speech, assembly, and association and violate the Fourth Amendment right to privacy. Using facial recognition technology that misidentifies people of color may violate the Equal Protection Clause of the Fourteenth Amendment. Not disclosing use of facial recognition technology may violate a criminal defendant's due process.

The U.S. Commission on Civil Rights issued a report on "The Civil Rights Implications of the Federal Use of Facial Recognition Technology" in September 2024. The report addressed concerns about accuracy, oversight, transparency, discrimination, and access to justice. The Chair of the U.S. Commission on Civil Rights stated that "unregulated use of facial recognition technology poses significant risks to civil rights, especially for marginalized groups who have historically borne the brunt of discriminatory practices."

The European Union's Artificial Intelligence Act (EU AI Act) recognizes that mass surveillance may dissuade the exercise of fundamental rights and further the biased and discriminatory effects of biometric identification and facial recognition technologies. Article 5 of the EU AI Act prohibits the creation and expansion of facial recognition databases that scrape facial images from the internet or CCTV footage. In addition, the EU AI Act prohibits real-time biometric identification in public spaces, although it contains carve outs for law enforcement and private actor usage.

As of January 2025, fifteen states have laws limiting police use of facial recognition technology. As of March 2025, seven states, including Illinois, have passed biometric legislation. Both Montana and Utah enacted a warrant requirement for police use of facial recognition, and use is permitted only when investigating serious crimes. Montana prohibits the use of continuous facial surveillance.

2. Social Media Surveillance

The use of social media monitoring tools by law enforcement has increased with the proliferation of new tools created by private companies. Law enforcement can monitor social media by topic, group, and individual, find associations/networks, learn viewpoints, and identify credible threats.

In October and November 2020, Los Angeles police pilot tested a social monitoring tool called ABTShield. LAPD scanned two hundred million tweets for a list of words including protest, rally, police brutality, black lives matter, and election; and the LAPD tracked two anti-fascist groups and one account that provides updates on protests. ABTShield provided usernames associated with the flagged tweets.

ABTShield's collection of this data for law enforcement purposes likely violated Twitter's (now X's) developer terms and specifically a 2016 term prohibiting developers from allowing law enforcement to use Twitter data for surveillance purposes. X's prohibition only seems to apply to X's data and not public data (public data includes publicly available posts, a user's bio and publicly-stated location, display name, and username).

Dataminr is a company that offers its First Alert AI platform to law enforcement and news media. It used public Twitter data as its initial algorithm training data. Dataminr's AI platform "processes every public tweet in real time" and records events, which are shared with customers as automated alerts. Dataminr currently ingests information from one million publicly available data sources in 220+ countries. Twitter and the CIA were both investors in Dataminr

The Houston police uses Dataminr to "enhance situational awareness and provide real-time alerts for criminal, homeland security, and cyber-security purposes on all social media platforms." LAPD surveilled Gaza protests using Dataminr's AI platform in 2025 and police departments across the country surveilled Black Lives Matter protestors following the police murder of George Floyd using Dataminr. The Intercept found that Dataminr tracked and monitored activity related to anti-police violence rallies across the country. Dataminr's mostly white staff were tasked with identifying gang members for its law enforcement clients, but were not trained on how to identify a gang member. An Executive Vice President of Dataminr has said that relaying data to the police is not a form of surveillance; rather Dataminr is a news gathering tool.

ICE has been monitoring the social media of immigrants in furtherance of its detention and deportation efforts, including using SocialNet and GiantOak. ICE contracted with GiantOak from 2014-2022 to find derogatory social media posts about the United States. These posts were used to inform visa and immigration enforcement decisions. In 2025, DHS began monitoring the social media of immigrants, specifically for anti-semitism.

In March 2025, USCIS published a notice outlining its plan to collect social media usernames/handles on nine immigration forms. In addition, the U.S. is requiring student and exchange visitor applicants to provide a list of their social media usernames and handles used in the past five years on their visa forms and to change their privacy settings on all of their social media to public. (In October 2024, ICE entered into a six-month contract extension with Booz Allen to track foreign students and exchange visitors and provide data analytics support.)

ICE issued an RFP in November 2024 seeking a contractor to provide real-time and proactive threat mitigation and monitoring services because of the "increased level of external threat activity directed towards its senior leaders, personnel and facilities" on social media and online postings. The services will include performing analytics utilizing social and behavioral sciences to locate "dangerous individuals posing a possible threat." The contractor is expected to monitor and analyze behavioral and social media sentiment (i.e. are the social media comments about ICE positive, neutral, or negative), create psychological profiles on individuals, find any threatening deleted messages or content, and determine if individuals making threats have a potential for carrying out a threat (contractor will look for postings that include weapons, acts of violence, or empathy with a group that has violent tendencies).

Social media monitoring tools do not account for tone, speaker and context. When searching for a keyword, the tool reports all posts that include the word, including non-relevant posts. For example, the Jacksonville Sheriff's Office used Geofeedia to search for the word "bomb" (searches for black activist groups and abortion-related postings were also performed). Half of the sixty-seven alerts for "bomb" were not used for an incendiary device. Rather the posts described food, beer, and other things that people thought were awesome or were links to news articles that included the word "bomb".

Monitoring social media for limited scope purposes may promote public safety, such as tracking public disasters and credible threats of violence. However, law enforcement is using social media to track the movement of people and their speech, as well as to create dossiers on people. The lack of regulation can threaten First Amendment protected speech and association and violate privacy rights. For example, when DHS requires immigrants to disclose their social media account information and make their profiles public, DHS is able to surveil not only immigrants, but everyone they are connected to on social media, including U.S. citizens. Such surveillance may curtail First Amendment protected speech, as immigrants, and anyone connected to them, may self censor or avoid expressing views that are in conflict with the U.S. government. In addition, monitoring and analyzing social media sentiment could curtail speech against ICE or the government.

There is case law that supports First Amendment claims against the use of social media monitoring, including *Hassan v. City of New York*. Per the Brennan Center, surveillance that targets protected speech or disproportionately targets and harms a racial, ethnic, or religious group may give rise to First and/or Fourteenth Amendment challenges.

3. Geolocation Tracking

Geolocation data is being sold by data brokers, geolocation tracking companies, advertisers, and app developers to law enforcement. Many mobile apps request location access in order to use the app or certain features of the app. Most people agree to share their location without understanding that their location data may be transferred to the government or other third parties.

App developers add code known as software development kits (SDKs) provided by data brokers into their apps in exchange for the receipt of a per user payment. SDKs give data brokers access to location data when the app is open or whenever the phone is on. Data brokers include the geolocation data in their databases and/or sell geolocation data to law enforcement, AI developers, marketing firms, real estate companies, and other data brokers. As of 2024, the location intelligence market was estimated at $21.2 billion.

Owners of five or more Muslim prayer apps sold location data to data broker X-Mode, which then sold the location data to U.S. military contractors. A number of government agencies have purchased cell phone location information from private companies for the purposes of tracking, arresting and deporting people. A number of federal agencies, including ICE, CPB, FBI, DEA, and IRS, have purchased smartphone app geolocation data from at least five private companies, including Gravy Analytics (now Unacast), Venntel, Anomaly 6, X-Mode, and Babel Street without a warrant or binding court order.

Venntel, a subsidiary of Gravy Analytics, collected data associated with visits to places of worship, health-related locations, military sites, labor unions, and other locations and sold the data without obtaining verifiable user consent for government or commercial use. According to a 2024 Federal Trade Commission (FTC) complaint against Gravy Analytics and Venntel for unlawfully tracking and selling sensitive location data from users, Gravy Analytics claimed to "collect, process, and curate over seventeen billion signals from one billion mobile devices on a daily basis." In a January 2025 Order, the FTC prohibited Venntel from tracking and selling sensitive location data from app users in violation of the FTC Act. (In January 2025, Russian hackers claimed to have hacked Gravy, which is one of the largest known breaches of a geolocation mining company.)

The Department of Defense entered into a contract with Anomaly 6 in July 2024. Anomaly 6 harvests GPS pinpoints tracking at least three billion devices in real time and 2.5 trillion locational data points worldwide annually. Anomaly Six provides a Google Maps-style satellite view of the Earth and provides information about smartphone movements in an area selected by the user. In a marketing meeting with a social media surveillance company, Anomaly 6 demonstrated how it tracked the cellphones of National Security Agency and CIA personnel in the United States and Jordan and the cellphone of an individual aboard a Chinese nuclear submarine.

Geolocation tracking companies claim that cellphone location data is tied to device ID numbers instead of people's names, and, therefore, their companies do not violate an individual's privacy rights. However, tracking a cellphone for an extended period of time will likely result in information that will help to identify the phone's owner and places they visit and work, in addition to their associates.

The ACLU and the Center for Democracy & Technology are concerned that the federal government is violating Fourth Amendment protections by buying geolocation data from data brokers and private companies instead of obtaining a warrant for such data. In 2018, the Supreme Court ruled in *Carpenter v. United States* that law enforcement must obtain a search warrant from a judge in order to request personal location information from a cellphone company because of the "privacies of life" those records can reveal. Per *Carpenter*, location history "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." Legal experts argue that the logic in *Carpenter* should apply to the purchase of geolocation data from data brokers, app developers, and geolocation tracking companies.

4. License Plate Readers

Automatic License Plate Readers (ALPRs) are a surveillance tool used by law enforcement to identify vehicles driven by people suspected of criminal activity and terrorism, track stolen vehicles, issue tickets, assess tolls, and locate vehicles associated with missing persons, Amber alerts, or people in crisis. ALPRs are mounted on highway overpasses, attached to law enforcement vehicles, and mounted to street poles and lights. An ALPR's algorithm can predict future driving patterns and identify regular travel patterns. ALPRs can potentially track the movements of every car owner and all passengers in that car.

Law enforcement may own their own ALPRs or use ALPRs developed by private companies. It is common for law enforcement agencies with their own ALPRs to share data with law enforcement within

their state or out of state. A hotlist of license plates can be uploaded into the ALPR and law enforcement will receive an alert when the plate is scanned, thereby tracking vehicles in real time. Vigilant Solutions (a subsidiary of Motorola Solutions) and Flock Safety are the two most used ALPR vendors.

Flock Safety reads twenty billion plates per month and contracts with over 4,800 law enforcement agencies. It offers nationwide hotlist access through the FBI, National Crime Information Center, and 19+ state databases. Flock Safety offers AI products that can identify a vehicle without license plate data. Vehicle Fingerprint provides vehicle data, including make, color, type, and unique characteristics such as decals, bumper stickers, and rims. Flock Free Form is an AI-powered search feature where a user can provide partial details about a vehicle or a person (e.g. woman with red handbag). Flock Safety offers a National Lookup feature where users can access data from over 83,000 cameras/readers nationwide. Any municipal user opting into the National Lookup feature must agree to share the license plate data it collects with other users.

In 2024, Illinois enacted the Automated License Plate Recognition System Data Act. The Illinois law prohibits any user, including Illinois law enforcement, from selling, sharing, allowing access to, or transferring ALPR data to any state or local jurisdiction or out-of-state law enforcement for the purpose of enforcing a law that denies or interferes with a person's right to choose reproductive health care services or permits the detention or investigation of a person based on their immigration status.

A sheriff's office in Texas used Flock Safety's National Lookup feature in violation of Illinois law to locate a Texas woman who self-administered an abortion by accessing Mount Prospect, Illinois license plate data. In response, the Illinois Secretary of State instructed Flock Safety to shut off access for out-of-state authorities searching Illinois data for reasons impermissible under Illinois law.

State and local law enforcement are assisting ICE by performing immigration related searches in Flock Safety, sometimes in violation of state law. Data obtained by 404 Media between June 1, 2024 and May 5, 2025 indicated that state and local law enforcement performed more than 4,000 immigration related searches either at the request of or as an informal favor to federal agencies, even though some of these states and cities have sanctuary laws prohibiting such sharing. Ten law enforcement agencies in California, including the Los Angeles Police Department and San Diego Sheriff, violated a California law prohibiting the sharing of license plate reader data with other state and federal entities by sharing license plate reader data with ICE.

Prior to June of 2020, a number of U.S. agencies, including, Customs and Border Protection, Alcohol Tobacco Firearms and Explosives, Drug Enforcement Agency, and the U.S. Marshall Service, used Vigilant Solutions's ALPR data in furtherance of their arrest and detention initiatives. In June 2024, the U.S. Cybersecurity & Infrastructure Security Agency issued an advisory warning that Motorola Solutions' Vigilant License Plate Readers were exploitable, allowing unauthorized users access to sensitive information.

ALPR data led to two wrongful arrests in North Carolina, when police issued lookout alerts for vehicles with specific makes and models, but no license plate data. ALPRs have been used to "grid"

neighborhoods, which is when law enforcement drives up and down every street in an area to collect information on vehicles to use in future criminal investigations.

Griding has been used by the New York Police Department, Birmingham, Alabama Police Department, and the Oakland Police Department to target specific communities. Griding was used by police in Port Arthur, Texas (a town with a poverty and unemployment rate approximately double the state's average) to identify people with unpaid traffic ticket tickets. This tactic led to the disproportionate jailing of African Americans who could not afford those tickets; 1,500 people were jailed for unpaid traffic fines between 2009-2011, resulting in loss of employment and/or wages and further debt.

A Circuit Court in Norfolk, Virginia granted a criminal defendant's motion to suppress evidence obtained by ALPR cameras without a search warrant. The Court found that installing 172 cameras in the City of Norfolk and storing the personal data captured by the cameras was akin to a GPS device that requires a warrant. Per the Judge's ruling "the Commonwealth argues that vehicles are different because the defendant did not have a privacy expectation in the public sphere. However, a person does not surrender all Fourth Amendment protection by venturing into the public." In addition, the Institute of Justice filed a lawsuit in October 2024 against the City of Norfolk arguing that the use of the 172 ALPR cameras in Norfolk violates the Fourth Amendment's protection against unreasonable searches. The case is pending trial. Cities, such as Austin, Denver, Norfolk, and San Diego are considering discontinuing use of ALPRs.

By tracking movements of vehicles and ultimately people via ALPRs, law enforcement can collect sensitive information about anyone's life, including their associates, where they go for healthcare (and the type of healthcare), their participation in protests, where they work, and the religious institutions they visit (and their religion). This data is collected and stored without the knowledge or consent of the vehicle owner in violation of the Fourth Amendment's privacy protections. The disproportionate use of ALPRs in communities of color and immigrant communities coupled with poor or nonexistent data retention policies may result in a higher probability of long-term tracking of these communities.

5. Other Surveillance - Electronic Monitoring, Financial Tracking, and Mass Surveillance

ICE introduced its Alternatives to Detention (ATD) Intensive Supervision Appearance Program (ISAP) in 2004 to track non-detained immigrants utilizing electronic and biometric monitoring tools. Individuals in ATD-ISAP are monitored using ankle/wrist monitors, telephonic reporting, and the SmartLINK app, a biometric check-in application. Non-detained immigrants must share a photo of themselves through the SmartLINK app to verify their identity and provide their location. DHS has stated that the photos are not shared or stored with any other agencies; however, ICE can take over the functions of a non-detained immigrant's phone via the SmartLINK app. BI Incorporated provides this technology to ICE and is a subsidiary of The GEO Group, the private prison company that operates at least 16 jails on behalf of ICE.

The Transaction Record Analysis Center (TRAC), a non-profit associated with the Arizona Attorney General's Office, provides more than six hundred federal, state, and local law enforcement agencies with access to a database that contains information about wire/money transfers sent via Western Union and other companies that are used by immigrants to send money to family abroad. ICE has been the top user of the database and has issued "customs summons" to wire transfer companies requiring them to send

wire transfer data to TRAC. (Custom summons are supposed to be limited to investigations related to merchandise imports and customs duties.) TRAC was established in 2014 as a result of a settlement agreement between Western Union and the Arizona Attorney General's Office to combat cross-border money laundering and drug trafficking.

Customs and Border Protection is using various technologies to track people, phones, and vehicles. CBP uses drones for border security, but has been deploying drones during protests taking place far from the border, including at the ICE detention facility outside of Chicago. The footage can be run through facial recognition tools. CBP has contracted with Anduril Industries for the installation of three hundred autonomous surveillance towers that use AI to detect and track the movement of people along and across the US border. In November 2025, the FBI published a RFI for AI technology capable of operating drones that can perform facial recognition, scan license plates, and detect weapons. These technologies are mass surveillance tools that target the movements of everyone in the U.S., not just immigrants or criminals.

State and local law enforcement are increasingly using AI software by Veritone, including Veritone Track, which tracks individuals and vehicles via recorded videos. Veritone Track analyzes the videos to attempt to identify individuals via body size, gender, hair color, clothing, and gait. The Executive Office for United States Attorneys, a sub-agency of the DOJ, uses Veritone Track. According to Veritone, users are not permitted to search for people by skin color. Veritone Track will soon track persons and vehicles using live video feeds.

Law enforcement is likely using Veritone Track as a way to get around facial recognition technology bans and restrictions. The ACLU has stated that use of Veritone Track raises the same privacy concerns as the use of facial recognition technology. The ACLU is concerned that law enforcements' use of Veritone Track, or similar tracking technologies, will increase because of the increasing restrictions on law enforcement use of facial recognition technology. Some states and municipalities ban use of biometric data such as faces, gait, and fingerprints, which may limit some uses of Veritone Track, but law enforcement still may be able to search for persons based on other physical attributes, such as body size.

In the Fall of 2025, Homeland Security Investigations, DHS´investigative unit, contracted with the Israeli skyware company Pararon Solutions for use of its remote cellphone hacking tool. The tool provides access to device location data, text messages, and photographs in real time and has the ability to hack into encrypted applications.

B. Predicting Future Outcomes

1. Crime Prediction Algorithms / Predictive Policing

Predictive analytics make predictions about future outcomes using historical data combined with statistical modeling, data mining, and machine learning. Predictive policing algorithms are used to predict and prevent future crimes by analyzing large data sets, including historical crime data. Predictive policing algorithms predict the location of a crime and whether a person is likely to commit a crime or be a crime victim and can be used to make pretrial detention decisions.

ICE issued an RFI in November 2024 seeking vendors to augment its Enforcement Removal Operations Law Enforcement Systems and Analysis (LESA) division by providing predictive analytics and developing AI tools to collect new data and improve forecasting methodologies and scenario-planning capabilities. The selected contractor will be expected to improve LESA's geospatial capabilities, use ICE's machine learning prediction model the Hurricane Score, and improve automated data gathering.

The Chicago Police Department (CPD) used two predictive policing programs from 2012-2020, the Strategic Subject List (the "heat list") and the Crime and Victimization Risk Model. These models predicted the likelihood that an individual would commit gun violence or be a victim of gun violence. The list included the names of 399,000 people or every person arrested or fingerprinted in Chicago starting in 2013. One hundred fifty-three people were given the highest risk score (500). Approximately half of the people with the highest risk score never had been arrested for illegal gun possession or unlawful use of a weapon, but 87% had been arrested for a violent, unspecified offense. The Chicago Office of the Inspector General assessed the model and found the risk scores unreliable because the scores were not regularly updated, the data quality was poor, CPD lacked controls for use of the risk scores, and CPD overrelied on arrest records even where there was no further arrest or arrests did not lead to convictions.

Algorithms are complex and make decisions based on patterns and data undisclosed to users and the persons identified by the crime prediction model. The data used to train the algorithms is often outdated and inaccurate and derived from biased and unlawful policing practices, including data derived from overpoliced areas. There has been concern about predictive policing models on a federal level. Since 2021, U.S. Senators have been asking the DOJ to halt grants for predictive policing systems until the DOJ can ensure that use will not result in discriminatory impact, the systems are subject to independent audits that assess accuracy, validity, and risks, and due process is provided to affected individuals.

In addition, crime prediction algorithms do not set forth the reasoning supporting decisions on policing or detention. The user doesn't know how the model arrived at its conclusion, and this lack of transparency is known as a "black box." Legal experts argue that crime prediction algorithms violate due process because detention predictions are not justified, neutral decisionmakers are not involved in the process, and the detained, specifically in the immigration context, are not provided the opportunity to represent themselves and present factual information. Some legal experts argue that predictive policing violates the Fourth Amendment, which requires reasonable suspicion for a stop. There is a concern that predictive analytics may make it easier for law enforcement to meet the reasonable suspicion standard, justifying more stops. In addition, there is evidence that predictive policing perpetuates racial bias, entrenches discriminatory practices, and undermines trust in law enforcement. Relying on historical criminal data negatively affects communities that have been historically overpoliced. Further, crime prediction algorithms are easily manipulated by political actors, with biased inputs or prompts leading to biased outputs.

Since algorithms are trade secrets, companies have not been transparent about how their AI works. There is a movement in explainable AI (XAI) which would make AI models more transparent and explain why and how a decision is made.

2. Risk Assessment AI Tools

Risk assessment tools use algorithms to predict outcomes and are used in pretrial release, sentencing, and probation. These tools can predict whether a person poses a public safety risk or will fail to appear in court. The criminal law system argues these tools are objective and unbiased, unlike human decisionmaking.

Recidivism prediction tools are used to make a decision about a person's civil liberties. For example, if a person is being considered for release from custody or jail, the tools will predict the likelihood of that person committing a crime and whether that person should be surveilled using electronic monitoring or check-ins. The person is being punished for a crime never committed. Recidivism prediction algorithms are trained on historical, biased criminal law data and learn the patterns of the types of people who are regularly incarcerated (disproportionately people of color).

Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), developed by Northpoint Institute for Public Management, Inc., is an algorithm that has been used by law enforcement since 1998. COMPAS predicts a person's risk of committing a misdemeanor or felony within two years of the assessment based on an individual's demographics and criminal record. A number of universities have criticized the accuracy of the predictions, with Dartmouth researchers finding that COMPAS did not outperform the human baseline on recidivism prediction. The Dartmouth analysis also found that the false positive rate (a person did not offend but was classified as a high risk) was higher for African American than white defendants and that the software could magnify existing biases in the criminal law system. A similar pretrial risk assessment tool is The Public Safety Assessment.

Beginning in 2013, ICE began using the Risk Classification Assessment (RCA), an algorithmic risk assessment tool used to evaluate a detainee's eligibility for release based on factors that measure flight risk and danger to public safety. In 2015, the U.S. Office of the Inspector General found that the RCA was not effective in determining which immigrants to release. In 2024, the U.S. Office of the Inspector General found that the RCA was not consistently used to detain or release individuals. This tool is not included in DHS's 2024 AI use case list, but not all AI use cases are included on the DHS list.

In or around 2020, ICE began using a machine learning model called the Hurricane Score to predict an immigrant's likelihood of compliance with ICE's Alternatives to Detention (ATD) Intensive Supervision Appearance Program (ISAP). The Hurricane Score is fed information about an individual's supervision and compliance history, benefits, caregiver status, immigration stage, and criminal history. The Hurricane Score determines the probability of compliance (or likelihood to abscond) using patterns it learned from inactive ATD-ISAP case data. Depending on the score, ICE may require electronic monitoring, telephonic monitoring, and/or biometric check-ins.

The same legal concerns that apply to predictive policing apply to risk assessment AI.

C. Investigative and Intelligence Databases

Investigative databases and intelligence databases centralize data and offer AI data analytics that provide insights, such as crime trends and "hidden" relationships between groups. The databases developed by data brokers contain massive amounts of personal data the data brokers have purchased or collected and may integrate with other company owned systems. In addition, law enforcement may be able to upload data from disparate sources to these databases. These databases can identify patterns and connections in support of investigations and provide real-time access to license plate data and arrest records.

DHS uses the Thomson Reuters CLEAR investigative platform. Both ICE and DHS use LexisNexis Risk Solutions´Accurint for Law Enforcement, which provides access to information about an individual's assets, relatives, and associates. Accurint Virtual Crime Center is designed to aid law enforcement in making data-driven operational decisions using analytics and provides access to data from over 10,000 sources, including police agencies nationwide. Law Enforcement can obtain identity data, retrieve jail booking photos, reveal non-obvious connections between people, image match, obtain trend insights, and map patterns of movement. Using Accurint Trax, law enforcement can "conduct pattern of life analysis" by observing calls in real-time and performing call detail record analysis.

ICE uses the "Justice Intelligence" service created by Appriss Insights (acquired by Equifax in 2021), which provides users access to data from over 2,800 jails and correctional facilities and real time alerts when an individual being tracked is released from jail. ICE is using Justice Intelligence to track and locate immigrants in sanctuary cities. Per its Justification for using the Justice Intelligence service, ICE stated that: "due to policy or legislative changes, ERO [Enforcement and Removals Office] has experienced an increase in the number of law enforcement agencies and state or local governments that do not share information about real time incarceration of foreign-born nationals with ICE."

According to Freedom of Information records regarding ICE's use of the Accurint tool, ICE conducted 1.2 million searches on individuals in the first seven months of its 2021 contract with LexisNexis, illustrating that ICE likely uses the Accurint tools to surveil all immigrants (not just ¨criminal¨ immigrants).

Homeland Security Investigations (HSI), a division of ICE that conducts mass immigration raids at workplaces, issued a 2024 RFP seeking a vendor to provide technology that is able to conduct unified searching across systems both internal and external to ICE and produce surveillance reports.

Some investigative databases can analyze data from mobile devices. These tools are taught to classify images into categories and use linguistic analysis to identify language patterns and sentiments in messages, emails, and documents. CBP issued an RFI in July 2025 for software designed to analyze forensically acquired electronic data from cell phones and other devices and perform data analytics on extracted data. As stated in the RFP, CBP is currently using "a wide variety of digital data extraction tools" and performed advanced searches on over 4,000 mobile devices in fiscal year 2024.

A declassified report released by the Office of the Director of National Intelligence (ODNI) in 2022 confirmed that intelligence agencies have been acquiring personal information on nearly everyone in the U.S. from commercial data brokers. Per the report:

> personal information *"can reveal sensitive and intimate information about the personal attributes, private behavior, social connections, and speech of individuals." Even subject to appropriate controls, commercially available information (CAI) can increase the power of the government's ability to peer into private lives to levels that may exceed our constitutional traditions or other social expectations."*

The report recommended that the intelligence community develop a set of standards for the purchase and use of online data. ODNI developed commercially available information usage rules in 2024 in response to this report, which required the intelligence community to assess the origin and sensitivity of CAI before use and establish usage requirements for sensitive CAI. Critics argue that the intelligence community's self-regulation will not result in privacy protections for individuals.

In an April 2025 RFP, ODNI indicated it wanted to centralize the procurement, access, and storage of CAI, including location data, digital transactions, facial recognition, and highly sensitive data. The potential vendor is required to acquire data regarding economic security, supply chain, critical infrastructure protection, agricultural, industry, and sentiment analysis from commercial data brokers.

A number of U.S. federal agencies are using tools provided by Palantir Technologies, a defense company, founded by the controversial Peter Thiel. Palantir Technologies has a number of subsidiaries, including Palantir USG, Inc., Palantir GSC Inc., Palantir International, and Palantir Engineering Israel Ltd.

Palantir Technologies is recognized for its ability to cross-reference vast amounts of data. It developed its reputation by analyzing multiple data streams to predict IED locations. It offers AI models to militaries and has an agreement with the Israeli Defense Ministry to support its war-related missions. In May 2025, the U.S. Department of Defense awarded Palantir USG a $795 million contract modification for its Maven Smart System used by the U.S. Army. The Maven Smart System integrates AI and machine learning to assess the battlespace and gathers and analyzes vast amounts of data to identify and prioritize "targets."

ICE has been using Palantir Technologies investigative solutions since 2011, and renewed its relationship by entering into a three year contract with Palantir Technologies in 2022 for its investigative case management software. In April 2025, ICE granted Palantir Technologies a contract to build a platform called Immigration OS to track migrant movements in real time, manage deportations, and monitor visa overstays.

The combined current award amount paid to Palantir Technologies since 2009 by all U.S. federal agencies is $1.3 billion; Palantir Technologies has contracted with HHS, USDA, DHS, VA, DOE, DOJ, DOD, and the State Department. The U.S. government has recently terminated contracts with its long-term surveillance contractors in cost-cutting measures, yet Palantir Technologies has partnered with these companies with the intention of accelerating AI across the federal government.

It has been reported that the Trump administration, specifically the IRS, is in communications with Palantir Technologies about creating a centralized database to unify data and track Americans. This unified database raises concerns about civil liberties and data weaponization, and members of the Senate Committee on Finance sent a letter to Palantir Technologies demanding answers to numerous questions.

Investigative and intelligence databases include personal data collected by unregulated, commercial data brokers. These databases contain data about potentially all people residing in the US and will likely impact privacy and civil liberties. Legal experts have argued that the Fourth Amendment should protect against the government's collection of CAI. In *Carpenter v. United States*, the court found that the government must obtain a warrant to collect highly sensitive information, specifically geolocation data. They also argue that the Electronic Communications Privacy Act (ECPA) should be used to protect privacy, as it was intended to evolve with new technologies.

IV. Regulatory Framework for AI Surveillance

The Trump administration favors the accelerated development and use of AI with little regard for its potential misuse and the lack of regulation. Regulating the use of AI and how personal data is procured and used by state and federal governments may help to protect the constitutional rights, civil liberties, and the privacy rights of citizens and immigrants and address concerns of bias, lack of transparency, fairness, harm, and accountability. The EU Artificial Intelligence Act and the UNESCO Recommendation on the Ethics of Artificial Intelligence are two regulatory models that should be reviewed in preparation for drafting federal and state regulations.

Below is a suggested regulatory framework for the use of AI technology by federal and state law enforcement:

- General Framework for Use
    - Limit first time use of a new product to a pilot period to evaluate advantages, harms and risks of use
    - Only use AI technology and personal data in compliance with applicable federal and state laws, including state sanctuary laws
    - Require human oversight and review of any predictions before decisions are made concerning arrest or detention. AI shall not be the decisionmaker
    - Prohibit law enforcement from purchasing/licensing use of any AI technology where the developer obtained training data via hacking, illegally from a user's account or device, or in violation of a contract, privacy policy, or terms of service
    - Limit personal data collection from the AI tool
    - Prohibit the seizure of all content on a personal/mobile device or online account
    - Prohibit the scraping of facial images from online public sources

- Vet and test products before licensing/purchase
    - Only purchase and use explainable AI tools
    - Assess the accuracy and quality of training data

    - Determine the origins of the training data - require developer to disclose information about the underlying training data
        - Ensure training data is representative
        - Do not use AI that was trained on biased or discriminatory data
        - Only use AI that was trained on data that was obtained legally and in compliance with applicable contracts, privacy policies, and terms of service
    - Test the AI tool before purchase/licensing for effectiveness, accuracy, and equity
    - Review the data security practices of the developer and vet the AI tool for vulnerabilities for breach/attack

- Framework for acceptable uses of AI technology
    - Only use personal data and predictions when relevant to an ongoing criminal investigation
    - Vet data, images, and predictions for accuracy and completeness before using in investigations or as the basis of arrest of detention
    - Warrants
        - Require a warrant or court order before arresting an individual
        - Require narrow warrants for access to digital devices and online accounts
        - Require a warrant or court order before obtaining license plate data from ALPRS and geolocation data from app developers, geolocation software developers, and advertisers
    - Obtain a court order when purchasing cellphone data from cellular service providers and data brokers

- Framework for prohibited uses of AI technology
    - Prohibit use as the primary investigative tool in solving crimes
    - Prohibit use to surveil protected classes and individuals exercising First Amendment rights, unless there is a demonstrable threat to public safety at an upcoming event
    - Prohibit the sharing of personal data and predictions with other federal and state agencies unless the receiving agency has jurisdiction, is engaged in an ongoing investigation, or will assist in stopping a demonstrable threat to public safety
    - Prohibit real-time biometric identification in public spaces; prohibit use of real-time biometric identification for surveillance
    - Prohibit use of AI for social scoring
    - Prohibit use of AI for the cognitive behavioral manipulation of people

- Required Policies
    - Maintain a risk assessment use policy, including purpose of use, procedures around the use, collection, retention, and sharing of personal data, risks of use, safeguards, and governance; an independent oversight authority should audit annually
    - Maintain a publicly available policy that includes the purpose of using the technology, general information about how the technology/algorithms work, practices, oversight, and why someone could be identified as a risk; review annually
    - Maintain a data governance policy, including use and retention policies; review annually

        - Limit the retention of personal data retention to the shortest time possible
        - Purge predictions and personal data not used in a criminal investigation or civil procedure
    - Re-evaluate impact on rights and potential for harms at the time of every update to AI model/algorithm
    - Maintain a data security policy to safeguard and protect personal data; review annually

- Transparency
    - Regularly assess / audit personal data and predictions for disparate impact, discrimination, bias, and privacy risks
    - Evaluate efficacy of using technology regularly
    - Report statistics related to use to public annually
    - Coordinate an annual independent, public audit of policy, procedures, and uses; audit for privacy and other rights violations
    - Disclose to the accused information about law enforcements´use of the AI technology during the investigation of the accused
    - Organize an AI oversight authority to regulate AI developers and protect the rights of individuals consisting of AI experts

- Training and Employee Use
    - Mandate employee training in advance of AI use and annually, include on bias in policing
    - Limit the number of users and prohibit the sharing of credentials; do not permit consultants to use AI surveillance technology
    - Prohibit use of fake (undercover) or impersonation social media and other online accounts for surveillance purposes

- Enforcement for Violations of Framework
    - Include enforcement mechanisms, including right to civil action, injunctive relief, employee administrative remedies, and exclusion of evidence
    - Mandate liability for the AI developer and any contractors assisting the deployment of an AI system for violating any provision of the future regulation

An AI regulation must include the following AI developer requirements:

- Inform the public about how the AI technology works
- Require all companies to regularly assess their algorithms for accuracy, disparate impact, discrimination, and bias and publish such findings
- Require disclosure of all sources of personal data to the public
- Annual submission of algorithms and methods for predictions to the AI oversight authority
- Require the development of a framework for collection, processing, and transfer of biometric information, including the requirement to obtain consent for every facial image the developer makes available to the government and other third parties

- Annually require app developers to disclose use of software development kits (SDKs) and the names of third parties with which they share data

V. Comprehensive Privacy Law

Private companies profit off the collection, scraping, compilation, and analysis of personal data and highly sensitive data. Data brokers have compiled data on millions of Americans by using cookies, searching through public records (such as court, vehicle, and property tax records) and buying data from insurance companies, social media platforms, app developers, internet service providers, and other companies without limitation.

Data brokers generally do not provide notice or obtain informed consent before procuring, using, or transferring personal data. Most individuals do not read complicated privacy policies and are likely uninformed that their personal data may be sold for secondary uses. Further, the privacy practices of these companies often are not sufficient to protect individuals' privacy given the significant amount of Commercial Available Information purchased and used by law enforcement for AI surveillance.

Transparency regarding how personal data is collected and used is just as important as transparency regarding the use of AI. As recognized by the Electronic Privacy Information Center, a comprehensive privacy law is the foundation for AI regulation. A U.S national data privacy law should be no less restrictive than the General Data Protection Regulation (GDPR) to give U.S. residents control over how their personal data is collected, stored, processed, transferred and destroyed. Data should not be collected without consent, and corporations and organizations should use and process personal data only in compliance with applicable law and a lawful basis (as defined under the GDPR).

Nineteen states have enacted state-wide privacy laws. Some of the most recent laws address privacy harms, such as profiling (Minnesota), naming the third parties to which a business may sell personal data (Rhode Island), and requiring notice when using tracking technologies (New Jersey). Montana was the first state to close the data broker loophole with SB 282. In Montana, government entities may not purchase geolocation data, electronic communications, communications from a tracking device, information on electronic funds transfer, sensitive data, and other information without a search warrant, investigative subpoena, or consent of the owner of the electronic device. Sensitive data includes information about a person's private life, personal associations, religious affiliation, health status, citizenship status, biometric data, and precise geolocation.

Closing the data broker loophole is a path to ensure that the government does not sidestep the Fourth Amendment by buying personal data from data brokers. The Fourth Amendment is Not For Sale Act was introduced in April 2021 by both a Republican and a Democratic U.S. Senator and cosponsored by 18 other U.S. Senators. It was reintroduced in 2024 with a companion bill in the U.S. House. The Act passed the U.S. House in Spring 2024, but did not make it to the U.S. Senate floor. The Act sought to add a provision to the Electronic Communications Privacy Act to prohibit government agencies from buying specified personal data, including communications, content, and geolocation data from a number of commercial entities and prohibited purchasing "illegitimately obtained information," i.e., information obtained through unauthorized access to a device or online account or in violation of a website owner's or

social media provider's terms of service or privacy policy. Those critical of the Act suggest a future version of the Act should address biometric, health, and other sensitive information.

Below is a list of general provisions for inclusion in federal and state privacy laws:

- Principles
    - Data minimization - the collection and use of personal data for narrow, specified purposes and the storage of that data for a limited period of time
    - Lawful bases for data processing (Article 6 of the GDPR)
    - Consent - prohibit private companies scraping the Internet and apps for personal data
    - Restrict the transfer of sensitive personal data or information

- Rights of Data Subjects
    - Enact rights, including access, rectification, erasure, restriction on processing, objection, and data portability
    - Right to erasure or right to be forgotten
    - A central resource for individuals to request the deletion of their data from all private companies
    - The right to opt out of automated decisionmaking and predictive profiling

- Oversight
    - Organize a federal Data Protection Agency to regulate the data broker industry
    - Organize a centralized authority where individuals can request deletion of their personal data and permanent opt-outs for the sale of their personal data from specific or all vendors (avoid individuals from being required to contact every company that possesses their personal data separately)
    - Create data intermediaries per state to manage access to personal data on behalf of individuals

- Data Broker Regulations
    - Regulate advertising and privacy policies, including prohibiting inaccurate language around privacy protections/practices (i.e. prohibit companies from stating it protects data when it scraped data from the Internet or that it is performing newsgathering services when it is a surveillance company)
    - Prohibit federal and state governmental agencies from sharing personal data with private companies, including data brokers and AI developers
    - Require companies to practice data minimization
    - Require data brokers processing location data to register with states (i.e. California and Vermont laws require such disclosure)
    - Require Clearview and other facial recognition technology companies to adopt opt-in consent models and to delete facial images automatically where opt-in was not obtained
    - Require all technology developers collecting personal data, location data, social media data, cellphone data, etc. to adopt opt-in models of consent

13 February 2026
Angela Baluk, Esq.
Member, Chicago Council of Lawyers Civil Liberties Committee