Das kommerzielle Panoptikum: Eine erschöpfende Analyse des Ökosystems des Datenhandels und der Umgehung des Vierten Verfassungszusatzes durch US-Regierungsbehörden

Zusammenfassung

Die vorliegende Forschungsarbeit bietet eine umfassende Analyse der symbiotischen Beziehung zwischen der kommerziellen Datenindustrie und den Strafverfolgungs- sowie Nachrichtendiensten der Vereinigten Staaten, mit einem spezifischen Fokus auf das Department of Homeland Security (DHS) und Immigration and Customs Enforcement (ICE). Im Zentrum der Untersuchung steht die systematische Umgehung des Vierten Verfassungszusatzes (Fourth Amendment), der Bürger vor unangemessenen Durchsuchungen und Beschlagnahmungen schützt. Durch die Nutzung der sogenannten "Drittparteien-Doktrin" (Third-Party Doctrine) und die Interpretation von Regierungsbehörden als Marktteilnehmer hat sich ein rechtliches und operatives Schlupfloch etabliert: Behörden erwerben sensible personenbezogene Daten – von Bewegungsprofilen bis hin zu Versorgungsrechnungen – auf dem freien Markt, anstatt richterliche Beschlüsse zu erwirken.

Der Bericht dokumentiert detailliert die Mechanismen, durch die Datenbroker wie **LexisNexis (RELX)**, **Equifax**, **Venntel** und **Palantir** riesige Mengen an Verbraucherdaten aggregieren, verknüpfen und als "Intelligence-Produkte" an den Staat verkaufen. Besondere Aufmerksamkeit gilt dabei der technologischen Evolution zwischen 2024 und 2026, in der die Integration von Künstlicher Intelligenz (KI) und prädiktiven Analysetools wie dem **Hurricane Score** und **ELITE** (Enhanced Leads Identification & Targeting for Enforcement) den Übergang von einer reaktiven Ermittlung zu einer proaktiven, algorithmischen Überwachung markiert.

Diese Analyse stützt sich auf eine Vielzahl von Regierungsdokumenten, Vertragsdaten, investigativen Berichten und juristischen Fachanalysen, um aufzuzeigen, wie tiefgreifend die Privatisierung der Überwachungsinfrastruktur die verfassungsrechtlichen Schutzmechanismen ausgehöhlt hat.

---

1. Einleitung: Vom Überwachungsstaat zum Überwachungsmarkt

In der historischen Betrachtung staatlicher Überwachung dominiert oft das Bild zentralisierter staatlicher Apparate, die Informationen durch Zwang, Wanzen oder verdeckte Ermittler sammeln. Das 21. Jahrhundert hat jedoch einen Paradigmenwechsel eingeleitet, der diese Mechanismen grundlegend transformiert hat. Der moderne amerikanische Überwachungsapparat ist nicht mehr primär ein Produzent von Daten, sondern ein Konsument. Er stützt sich auf eine privatwirtschaftliche Infrastruktur, die ursprünglich für Marketing, Kreditrisikoprüfung und Betrugsbekämpfung entwickelt wurde, nun aber nahtlos in die nationale Sicherheitsarchitektur integriert ist.

Die US-Behörde für Einwanderung und Zoll (ICE) sowie der Zoll- und Grenzschutz (CBP) stehen an der Spitze dieser Entwicklung. Da sie operativ im Inland tätig sind, unterliegen sie theoretisch den strengen Auflagen des Vierten Verfassungszusatzes. Praktisch jedoch nutzen sie ein juristisches Vakuum, das als "Fourth Amendment Loophole" bekannt ist. Dieses Schlupfloch erlaubt es der Exekutive, den richterlichen Vorbehalt zu umgehen, indem sie argumentiert, dass Daten, die legal käuflich zu erwerben sind, keiner richterlichen Anordnung bedürfen.

Die Implikationen dieses Wandels sind tiefgreifend. Während der Staat an verfassungsrechtliche Grenzen gebunden ist, operiert der private Datenmarkt weitgehend unreguliert. Wenn der Staat zum Kunden wird, importiert er die Kapazitäten des privaten Sektors – einschließlich der Fähigkeit, Bewegungsprofile von Millionen Menschen in Echtzeit zu verfolgen – ohne die verfassungsrechtlichen Kontrollen zu importieren, die für staatliches Handeln vorgesehen sind. Dieser Bericht wird die Anatomie dieses "kommerziellen Panoptikums" sezieren, von den rechtlichen Fundamenten über die technischen Sammelmechanismen bis hin zu den operativen Konsequenzen für die betroffenen Individuen.

---

2. Der verfassungsrechtliche Rahmen und das "Kauf"-Schlupfloch

Um die Dynamik des kommerziellen Datenhandels im Regierungskontext zu verstehen, ist eine detaillierte Auseinandersetzung mit der US-Verfassungsjurisprudenz unerlässlich. Der Vierte Verfassungszusatz schützt das "Recht des Volkes, in seinen Personen, Häusern, Papieren und Wirkungen vor unangemessenen Durchsuchungen und Beschlagnahmungen sicher zu sein." Historisch gesehen erforderte dies einen richterlichen Durchsuchungsbeschluss (Warrant),

der auf einem hinreichenden Tatverdacht (Probable Cause) basieren muss.

2.1 Die Doktrin der Dritten Partei (Third-Party Doctrine)

Das juristische Fundament, auf dem der heutige Datenhandel mit Behörden ruht, wurde in den 1970er Jahren durch den Obersten Gerichtshof (Supreme Court) gelegt. In zwei wegweisenden Entscheidungen etablierte das Gericht die **Third-Party Doctrine**:

1. **United States v. Miller (1976):** In diesem Fall entschied das Gericht, dass Bankkunden keine legitime Erwartung auf Privatsphäre bezüglich ihrer Finanztransaktionsdaten haben. Die Begründung lautete, dass diese Aufzeichnungen Eigentum der Bank seien und der Kunde das Risiko der Weitergabe eingehe, sobald er diese Informationen freiwillig an die Bank übermittle.[1]
2. **Smith v. Maryland (1979):** Diese Entscheidung weitete das Prinzip auf Telefondaten aus. Das Gericht befand, dass die Nutzung eines Telefons und das Wählen einer Nummer eine freiwillige Übermittlung von Informationen an die Telefongesellschaft darstelle. Daher sei die Installation eines "Pen Register" (ein Gerät zur Aufzeichnung gewählter Nummern) durch die Polizei ohne richterlichen Beschluss zulässig.

Diese Doktrin basierte auf der Annahme einer *freiwilligen* Preisgabe. Im analogen Zeitalter war es durchaus möglich, ohne Bankkonto oder Telefon zu leben, wenngleich schwierig. Im digitalen Zeitalter ist die "Freiwilligkeit" jedoch zur Fiktion geworden. Nahezu jede Interaktion des modernen Lebens – vom Einschalten des Lichts (Versorgungsdaten) über das Mitführen eines Mobiltelefons (Standortdaten) bis hin zur Erwerbstätigkeit (Gehaltsabrechnungsdaten) – generiert digitale Spuren bei Dritten.

2.2 Carpenter v. United States: Ein Riss im Fundament

Im Jahr 2018 fällte der Supreme Court im Fall **Carpenter v. United States** ein Urteil, das die Anwendbarkeit der Third-Party Doctrine im digitalen Zeitalter einschränkte. Das Gericht entschied, dass die Regierung einen richterlichen Beschluss benötigt, um historische **Mobilfunkstandortdaten (CSLI - Cell Site Location Information)** von Mobilfunkanbietern anzufordern.[2]

Chief Justice John Roberts argumentierte, dass Mobiltelefone heutzutage "fast ein Merkmal der menschlichen Anatomie" seien und ihre Standortdaten einen so tiefen Einblick in die "Privatheit des Lebens" gewähren, dass die Third-Party Doctrine hier nicht greife. Das Urteil erkannte an, dass Nutzer eine "angemessene Erwartung an Privatsphäre" in Bezug auf ihre physischen Bewegungen über einen längeren Zeitraum haben, selbst wenn diese Daten technisch gesehen bei einem Dritten (dem Mobilfunkanbieter) liegen.

2.3 Die Unterscheidung zwischen "Zwang" und "Kauf"

Trotz der Tragweite von *Carpenter* ließen die Richter eine entscheidende Hintertür offen. Das Urteil bezog sich explizit auf die **zwangsweise Herausgabe** (compelled disclosure) von Daten durch den Staat. Es äußerte sich nicht zur **käuflichen Erwerbung** derselben Daten auf dem freien Markt.

Genau in dieser Lücke operieren Behörden wie ICE, CBP und FBI heute. Ihre juristische Argumentation lautet:

- Wenn die Regierung Daten mittels einer Vorladung (Subpoena) oder Anordnung erzwingt, handelt sie hoheitlich und unterliegt dem Vierten Verfassungszusatz (nach *Carpenter*).
- Wenn die Regierung jedoch Daten kauft, tritt sie als Marktteilnehmer auf, genau wie ein privates Unternehmen. Da der Verkäufer (der Datenbroker) die Daten freiwillig verkauft und der Nutzer sie (nach Lesart der Behörden) freiwillig an die App oder den Dienstleister übermittelt hat, finde keine "Durchsuchung" im verfassungsrechtlichen Sinne statt.[3]

Diese Unterscheidung führt zu der paradoxen Situation, dass die Polizei einen Richter überzeugen muss, um Standortdaten von Verizon oder AT&T zu erhalten, dieselben (oder präzisere) Daten jedoch ohne richterliche Kontrolle von einem Broker wie Venntel kaufen kann.

2.4 Das Problem der "State Action"

Ein weiteres verfassungsrechtliches Hindernis für Kläger ist die Doktrin der "State Action" (Staatliches Handeln). Der Vierte Verfassungszusatz bindet nur den Staat, nicht private Akteure. Wenn ein Datenbroker Daten sammelt, gilt dies als "private Durchsuchung", die verfassungsrechtlich unbedenklich ist. Damit der Kauf dieser Daten durch den Staat verfassungswidrig wird, müsste nachgewiesen werden, dass der Broker als "Agent" oder "Instrument" der Regierung handelte – etwa, weil die Regierung die Sammlung aktiv angeordnet oder dazu angestiftet hat.[3]

Da der Markt für diese Daten jedoch primär kommerziell getrieben ist (Werbung, Kreditrisiko), argumentieren Gerichte oft, dass die Sammlung unabhängig vom Interesse der Regierung stattgefunden hätte. Die Regierung erntet lediglich die Früchte einer privaten Überwachungsökonomie.

---

3. Das Ökosystem der Datenbroker: Struktur und Mechanismen

Der Markt für kommerzielle Daten ist ein undurchsichtiges Geflecht aus Tausenden von Unternehmen, die Daten sammeln, aggregieren, veredeln und verkaufen. Für die Zwecke der Regierungsüberwachung lässt sich dieses Ökosystem in vier Hauptkategorien unterteilen, die jeweils unterschiedliche Aspekte des menschlichen Lebens abdecken:

1. **Identitäts- und Rechtsdaten:** Fokussiert auf Namen, Adressen, Beziehungen und rechtliche Historie (z.B. LexisNexis).
2. **Finanz- und Versorgungsdaten:** Fokussiert auf Kreditwürdigkeit, Beschäftigung und Infrastrukturnutzung (z.B. Equifax).
3. **Standort- und Bewegungsdaten:** Fokussiert auf physische Bewegungen via GPS und Ad-Tech (z.B. Venntel, Babel Street).
4. **Integrationsplattformen:** Software, die diese Datenströme zusammenführt (z.B. Palantir).

Die folgende Tabelle bietet eine Übersicht über die primären Akteure und ihre Relevanz für ICE:

Unternehmen	Produkt/Dienstleistung	Datentyp	Primäre Nutzung durch ICE/DHS
RELX (LexisNexis)	Accurint, LexID	Öffentliche Register, Kredit-Header, Haftdaten, LPR (Kennzeichen)	Erstellung umfassender Personenprofile; "Virtual Crime Center". [4]
Equifax	The Work Number, NCTUE	Beschäftigungsdaten, Gehaltsabrechnungen, Versorgungsrechnungen	Lokalisierung von Arbeitsplätzen für Razzien; Adressfindung über Strom/Wasser. [6]
Venntel (Gravy Analytics)	Location Data Feed	Mobile GPS-Daten (via Apps)	Historische Bewegungsprofile; Grenzüberwachung; Identifikation von "safe houses". [8]

Babel Street	Babel X / Locate X	OSINT, Geofencing	Analyse sozialer Medien; Verfolgung von Bewegungen in Echtzeit. [8]
Palantir	FALCON, ICM, ELITE	Datenanalyse-Plattform	Das "Betriebssystem" der Abschiebung; Verknüpfung isolierter Datensilos. [10]
Appriss Insights	VINE / Justice Intelligence	Echtzeit-Haftdaten (Jail Booking)	Umgehung von Sanctuary-City-Gesetzen durch Benachrichtigung bei Haftentlassung. [5]

---

4. Tiefenanalyse: LexisNexis und das "Virtuelle Kriminalamt"

LexisNexis Risk Solutions, eine Tochtergesellschaft des anglo-niederländischen Konzerns RELX, ist weit mehr als ein Anbieter juristischer Datenbanken. Das Unternehmen fungiert de facto als privatisiertes Nachrichtendienst- und Fahndungszentrum für US-Behörden.

4.1 Accurint und LEIDS

Das Flaggschiffprodukt für Strafverfolgungsbehörden ist **Accurint**. ICE greift auf dieses System oft über das Programm **Law Enforcement Investigative Database Subscription (LEIDS)** zu. Vertragsunterlagen belegen, dass das Department of Homeland Security zwischen 2005 und 2024 über **172 Millionen US-Dollar** an RELX und seine Tochtergesellschaften zahlte.[4] Ein spezifischer Vertrag aus dem Jahr 2021 sicherte ICE den Zugriff auf Accurint für bis zu 22,1 Millionen Dollar über fünf Jahre.[5]

Accurint ist keine einfache Suchmaschine. Es ist eine relationale Datenbank, die Milliarden von Datensätzen aus über 10.000 verschiedenen Quellen ("disconnected data") integriert.[5] Dazu gehören:

- Wählerverzeichnisse
- Immobilienregister
- Führerscheindaten
- Insolvenzbekanntmachungen
- Geschäftslizenzen
- Boots- und Fahrzeugregistrierungen

4.2 Die Macht der LexID: Identitätsauflösung

Der wahre Wert von LexisNexis liegt nicht nur in der Datenmenge, sondern in der Technologie der "Identitätsauflösung" (Identity Resolution). Das Unternehmen weist jeder erfassten Person eine eindeutige Kennung zu, die **LexID**. Diese deckt über **276 Millionen US-Konsumentenidentitäten** ab.[5]

Im Gegensatz zu einer Sozialversicherungsnummer (SSN), die statisch ist und von Undokumentierten oft nicht besessen wird, ist die LexID dynamisch und fehlertolerant. Sie verknüpft:

- Variationen von Namen (z.B. Schreibfehler in verschiedenen Akten).
- Veraltete Adressen.
- Telefonnummern und E-Mail-Adressen.
- Soziale Beziehungen (Mitbewohner, Nachbarn, Verwandte).

Für ICE ist dies von unschätzbarem Wert. Wenn eine Zielperson versucht, "unter dem Radar" zu leben, indem sie keine offiziellen Verträge abschließt, aber bei einem Verwandten wohnt, kann die "Link-Analyse" von LexisNexis diese Verbindung aufdecken. Ein ICE-Agent kann nicht nur nach der Person suchen, sondern ein "Comprehensive Person Report" generieren – ein Dossier, das teils über 40 Seiten lang ist und die gesamte Lebenshistorie, bekannte Assoziationen und finanzielle Verhältnisse offenlegt.[5]

4.3 Das Schlupfloch der Haftdaten: Appriss Insights

Ein besonders kritischer Aspekt der Strategie von LexisNexis war die Übernahme von **Appriss Insights**. Appriss betreibt das **VINE-Netzwerk** (Victim Information and Notification Everyday), ein System, das ursprünglich entwickelt wurde, um Opfer von Straftaten zu benachrichtigen, wenn der Täter aus der Haft entlassen wird oder verlegt wird.

ICE nutzt dieses System unter dem Namen **"Justice Intelligence"**, um Echtzeit-Informationen über Buchungen in lokalen Gefängnissen (Jails) zu erhalten.[5] Dies ist die technologische Antwort auf die "Sanctuary City"-Bewegung. Viele lokale Jurisdiktionen (z.B. Cook County, Illinois) untersagen ihrer Polizei die aktive Zusammenarbeit mit ICE oder die Meldung von Einwanderern ohne Papiere an Bundesbehörden. Da die Gefängnisdaten jedoch oft

automatisiert an Appriss/VINE gemeldet werden (zur Opferbenachrichtigung), kauft ICE diese Daten einfach von LexisNexis zurück. Wenn eine Zielperson wegen eines Verkehrsdelikts in einem "Sanctuary"-Gefängnis gebucht wird, erhält ICE durch "Justice Intelligence" einen Alarm und kann die Person bei der Entlassung abfangen, ohne dass die lokale Polizei kooperieren muss.[12]

---

5. Tiefenanalyse: Equifax, The Work Number und die Versorgungsdaten

Während LexisNexis das breite historische Profil liefert, bietet Equifax die taktische Präzision, die für den Zugriff ("Apprehension") notwendig ist. Equifax ist traditionell als Kreditbüro bekannt, doch seine unregulierten Datendienste sind für die Überwachung weitaus relevanter.

5.1 The Work Number: HR-Daten als Fahndungstool

The Work Number ist die größte zentrale Datenbank für Beschäftigungs- und Einkommensdaten in den USA. Sie wird direkt von Arbeitgebern gefüttert. Große Lohnabrechnungsdienstleister (wie ADP) übermitteln bei jeder Gehaltsabrechnung automatisch Daten an Equifax. Im Jahr 2024 enthielt die Datenbank Informationen zu über **190 Millionen Amerikanern**.[14]

- **Kommerzieller Zweck:** Ursprünglich gedacht für schnelle Bonitätsprüfungen bei Krediten oder Hypotheken.
- **Behördliche Nutzung:** ICE und FBI nutzen diese Datenbank, um den aktuellen Arbeitsplatz einer Zielperson zu identifizieren.
- **Operativer Wert:** Wohnadressen ändern sich oft oder sind verschleiert. Arbeitsplätze sind stabiler. Da die Daten mit jedem Gehaltsscheck ("pay period") aktualisiert werden [15], erhalten Agenten nahezu Echtzeit-Informationen darüber, wo sich eine Person tagsüber aufhält. Dies ermöglicht gezielte Festnahmen am Arbeitsplatz.

5.2 NCTUE: Das Versorgungsdaten-Schlupfloch

Eine der invasivsten, aber wenig bekannten Datenquellen ist der **National Consumer Telecommunications and Utilities Exchange (NCTUE)**. Dies ist eine von Equifax verwaltete Datenbank, die Zahlungsinformationen und Kontodaten von Versorgungsunternehmen (Strom, Wasser, Gas, Kabelfernsehen, Internet) enthält.

- **Der Zwang zur Datenpreisgabe:** Niemand kann ohne Wasser oder Strom leben. Um diese Dienste anzumelden, müssen Name und Adresse angegeben werden. Diese Daten fließen in den NCTUE.

- **Nutzung durch ICE:** Equifax verkauft Zugang zu diesen "Header-Daten" (Identitätsdaten) an Behörden. Ein Bericht des Georgetown Law Center on Privacy & Technology ("American Dragnet") ergab, dass ICE Zugang zu Versorgungsdaten von über **218 Millionen Individuen** hat.[16]
- **Erweiterte Analyse:** Dies ermöglicht ICE nicht nur die Lokalisierung einer Person, sondern auch die Analyse von Haushalten. Durch die Verknüpfung von Zählerdaten kann ermittelt werden, wer zusammenwohnt, selbst wenn keine familiäre oder rechtliche Beziehung besteht. Dies ist besonders relevant für das Aufspüren von Personen, die "off the grid" leben (keine Kreditkarten, keine Bankkonten), aber zwingend heizen oder Wasser verbrauchen müssen.

---

6. Tiefenanalyse: Standortdaten und die Fiktion der Anonymität

Der vielleicht kontroverseste Bereich des Datenhandels ist der Verkauf von präzisen Geolokalisierungsdaten ("Pattern-of-Life Data"). Hier wird das Versprechen der Anonymität systematisch ausgehebelt.

6.1 Die Lieferkette der Ad-Tech-Industrie

Unternehmen wie **Venntel** und **Babel Street** sammeln Daten nicht direkt, sondern kaufen sie aus dem Ökosystem der mobilen Werbung (Ad-Tech) auf.[8] Der Prozess verläuft typischerweise so:

1. **Die Quelle:** Ein Nutzer installiert eine App (Wetter, Spiel, Gebetbuch, Taschenlampe) und gewährt Zugriff auf den Standort.
2. **Das Leck (SDK):** Die App enthält ein Software Development Kit (SDK) eines Drittanbieters (z.B. X-Mode, Gravy Analytics), das den Standort abgreift und an Aggregatoren sendet.
3. **Der Bidstream:** Alternativ werden Standortdaten im Rahmen von "Real-Time Bidding" (RTB) Auktionen an Werbenetzwerke gesendet. Auch wenn kein Werbeplatz gekauft wird, werden die Daten (GPS, Device ID) oft gespeichert.
4. **Das Produkt:** Aggregatoren wie Venntel bündeln diese Billionen von Datenpunkten und verkaufen den Zugriff über Webportale an Regierungskunden.[9]

6.2 Die De-Anonymisierung

Behörden und Broker verteidigen diese Praxis mit dem Argument, die Daten seien "anonymisiert", da sie nicht mit Namen, sondern mit numerischen "Mobile Advertising IDs"

(MAIDs) verknüpft seien. Forschung und Praxis zeigen jedoch, dass diese Anonymität trivial zu brechen ist.[9] Durch die Analyse der Bewegungsmuster ("Pattern of Life") lässt sich fast jede Person identifizieren:

- Ein Gerät, das jede Nacht an Adresse A (Wohnort laut LexisNexis) und jeden Tag an Adresse B (Arbeitsplatz laut The Work Number) verweilt, gehört mit an Sicherheit grenzender Wahrscheinlichkeit der Person, die an Adresse A gemeldet ist.
- Sobald die Verbindung zwischen MAID und Name hergestellt ist (oft durch "Linkage"-Dienste von Brokern), kann die gesamte historische Bewegung der Person über Jahre hinweg rekonstruiert werden.

6.3 Operative Anwendung an der Grenze und im Inland

- **CBP:** Nutzt Venntel-Daten, um illegale Grenzübertritte in abgelegenen Gebieten zu identifizieren, indem nach Geräten gesucht wird, die sich abseits offizieller Grenzübergänge bewegen. Auch Tunnelbauaktivitäten können so durch die Analyse von Bewegungsmustern von Arbeitern und Fahrzeugen detektiert werden.[18]
- **ICE:** Nutzt die Daten im Inland, um "Frequented Locations" zu identifizieren. Wenn eine Zielperson untergetaucht ist, aber ihr Mobiltelefon weiter nutzt, verraten die aggregierten Standortdaten ihren neuen Aufenthaltsort, ohne dass eine aktive Ortung (die einen richterlichen Beschluss erfordern würde) notwendig ist.

---

7. Technologische Evolution: KI und Prädiktive Überwachung (2024–2026)

In den Jahren 2024 bis 2026 hat sich das Ökosystem durch die Integration von Künstlicher Intelligenz (KI) fundamental gewandelt. Die Phase der reinen Datensammlung wurde durch die Phase der **algorithmischen Zielerfassung** abgelöst.

7.1 Palantir und die generische KI: ELITE

Palantir Technologies bleibt das zentrale Betriebssystem der Datenfusion. Mit der Einführung von **ImmigrationOS** und dem Tool **ELITE** (Enhanced Leads Identification & Targeting for Enforcement) im Jahr 2025 wurde die Effizienz der Zielfindung massiv gesteigert.[11]

- **Generative KI:** ELITE nutzt Large Language Models (LLMs), um unstrukturierte Datenmengen lesbar zu machen. ICE verfügt über Millionen alter Akten, gescannter Polizeiberichte, handschriftlicher Notizen und Haftbefehle, die bisher nicht durchsuchbar waren. ELITE "liest" diese Dokumente, extrahiert Entitäten (Namen, Adressen, Beschreibungen) und normalisiert sie.

- **Address Confidence Score:** Das System erstellt Dossiers und weist Adressen einen Wahrscheinlichkeitswert ("Confidence Score") zu. Es sagt dem Agenten nicht nur, wo eine Person *könnte* sein, sondern berechnet die statistische Wahrscheinlichkeit ihres Aufenthalts basierend auf der Aktualität und Konsistenz der Datenquellen (z.B. frische Stromanmeldung vs. alter Führerschein).
- **Fehlende Aufsicht:** Berichten zufolge hat DHS das Tool ELITE als "nicht hochwirksam" (not high-impact) klassifiziert, wodurch es strengeren Auflagen zur Risikoprüfung und Bürgerrechtswahrung entzogen wurde, obwohl es direkt zur Planung von Razzien eingesetzt wird.[11]

7.2 Der Hurricane Score: Automatisierte Risikobewertung

Ein weiteres Beispiel für die algorithmische Wende ist der **Hurricane Score**, ein maschinelles Lernmodell, das von ICE im Rahmen des "Alternatives to Detention" (ATD) Programms eingesetzt wird.[20]

- **Funktionsweise:** Das Modell analysiert die Historie eines Migranten (Bewegungsmuster, Einhaltung von Meldepflichten), um einen Risikowert (Score 1-5) zu berechnen. Dieser Wert prognostiziert die Wahrscheinlichkeit, dass die Person "untertauchen" (abscond) wird.
- **Konsequenzen:** Ein hoher Score kann zu verschärften Überwachungsmaßnahmen führen, wie z.B. dem Tragen einer GPS-Fußfessel oder der erneuten Inhaftierung.
- **Black Box:** Da der Algorithmus von einem privaten Auftragnehmer (**B.I. Incorporated**, ein Unternehmen mit engen Verbindungen zur Privatgefängnis-Industrie) entwickelt wurde, sind die genauen Gewichtungsfaktoren unbekannt. Kritiker bemängeln, dass Faktoren wie Wohnortstabilität oder Einkommen einfließen könnten, was effektiv Armut kriminalisiert und rassistische Vorurteile (Bias) in den Algorithmus codiert.[22]

7.3 Biometrische Überwachung: Mobile Fortify

Seit Mai 2025 nutzen ICE und CBP die App **Mobile Fortify**, die Gesichtserkennung und Fingerabdruckabgleich im Feld ermöglicht. Agenten können Fotos von Personen auf der Straße machen und diese sofort gegen Datenbanken abgleichen. Trotz dokumentierter Fehlidentifikationen betrachtet ICE die Ergebnisse oft als "definitiv" für die Feststellung des Einwanderungsstatus.[21]

---

8. Legislative und gerichtliche Entwicklungen: Ein ungelöster Konflikt

Der Konflikt zwischen technologischer Machbarkeit und verfassungsrechtlichem Schutz hat den US-Kongress und die Gerichte erreicht, jedoch ohne bisherige definitive Lösung.

8.1 Der "Fourth Amendment Is Not For Sale Act"

Der wichtigste legislative Versuch, das Datenkauf-Schlupfloch zu schließen, ist der **Fourth Amendment Is Not For Sale Act** (H.R. 4639).

- **118. Kongress (2023-2024):** Der Gesetzentwurf passierte im April 2024 das Repräsentantenhaus mit überparteilicher Unterstützung. Er sah vor, Strafverfolgungs- und Nachrichtendiensten den Kauf von Abonnenten- oder Kundendaten zu untersagen, wenn für deren Erlangung im Wege des Zwangs ein Gerichtsbeschluss nötig wäre.[24] Der Senat verabschiedete das Gesetz jedoch nicht.
- **119. Kongress (2025-2026):** Der Status des Gesetzes bleibt in der neuen Legislaturperiode unsicher. Während Datenschützer aufgrund der KI-Entwicklung (ELITE, Hurricane Score) drängen, lobbyieren Polizeiverbände und Nachrichtendienste massiv dagegen. Sie argumentieren, ein Verbot würde sie "blind" machen gegenüber Bedrohungen, die für jeden privaten Marketinganalysten sichtbar seien.[26]

8.2 Gerichtliche Auseinandersetzungen

Die Gerichte ringen weiterhin mit der Anwendung von *Carpenter* auf den Datenkauf. Regierungsanwälte argumentieren konsistent, dass durch die öffentliche Verfügbarkeit der Daten (gegen Bezahlung) keine Privatsphärenerwartung bestehen könne. Bürgerrechtsorganisationen wie die **ACLU** und die **EFF** versuchen, die "State Action"-Doktrin anzugreifen, indem sie argumentieren, dass die Verflechtung zwischen Firmen wie Palantir und dem Staat so eng sei (durch eingebettete Analysten und maßgeschneiderte Tools), dass die Firmen als verlängerter Arm des Staates agieren und somit verfassungsrechtlich gebunden sein müssten.[28]

---

9. Fazit: Die Privatisierung des Vierten Verfassungszusatzes

Das hier analysierte Ökosystem markiert eine fundamentale Verschiebung in der Machtbalance zwischen Staat und Bürger. Der Vierte Verfassungszusatz wurde konzipiert, um staatliche Macht durch richterliche Kontrolle zu begrenzen. Der kommerzielle Datenhandel hebelt diesen Mechanismus aus, indem er die Ermittlungstätigkeit privatisiert.

Behörden wie ICE müssen keinen eigenen Überwachungsstaat aufbauen, da die

Privatwirtschaft diesen bereits aus Profitinteresse errichtet hat.

- **LexisNexis** liefert das Dossier.
- **Equifax** liefert den Arbeitsplatz und die Versorgungsdaten.
- **Venntel** liefert das Bewegungsprofil.
- **Palantir** und **B.I. Inc.** liefern die Zielanalytik und Risikobewertung.

Solange der Supreme Court oder der Kongress nicht explizit klarstellen, dass der *Kauf* sensibler Daten verfassungsrechtlich dem *Zwang* zur Herausgabe gleichgestellt ist, leben US-Bürger – und insbesondere Nicht-Staatsbürger – in einer Realität, in der Privatsphäre kein Recht mehr ist, sondern eine Dienstleistung, die an den Meistbietenden verkauft wird. Die Regierung muss lediglich den Marktpreis zahlen, um die verfassungsrechtlichen Hürden zu überspringen.

---

10. Anhang: Übersicht der Datenquellen und Auftragswerte

Anbieter	Datenkategorien	Geschätzter Auftragswert (DHS)	Behördenkunden
RELX (LexisNexis)	Öffentliche Register, Haftdaten, LPR	>$172 Mio. (2005-2024 total)	ICE, CBP, FBI, DHS [4]
Palantir	Analytik, Case Management (ICM)	>$30 Mio. (2025 ICE Vertrag)	ICE ERO, HSI [19]
Equifax	Beschäftigung (Work Number), Versorger	Intransparent (oft Subunternehmer)	ICE, FBI, SSA [6]
Venntel	Mobile Standortdaten (GPS)	~$800k - $1 Mio. jährlich wiederkehrend	CBP, ICE, DHS [9]

Clearview AI	Gesichtserkennung	$3,75 Mio. (Sept. 2025 Erweiterung)	ICE, FBI [29]

Ende des Berichts

Hinweis: Dieser Bericht synthetisiert Informationen, die bis Februar 2026 verfügbar waren, basierend auf Regierungsdokumenten, juristischen Analysen und investigativen Berichten aus dem bereitgestellten Forschungsmaterial.

Referenzen

1. A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance - Emory Law Scholarly Commons, Zugriff am Februar 14, 2026, https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1011&context=faculty-articles
2. Buying Data and the Fourth Amendment - Hoover Institution, Zugriff am Februar 14, 2026, https://www.hoover.org/sites/default/files/research/docs/kerr_webreadypdf.pdf
3. End-Running Warrants: Purchasing Data Under the Fourth ..., Zugriff am Februar 14, 2026, https://yalelawandpolicy.org/end-running-warrants-purchasing-data-under-fourth-amendment-and-state-action-problem
4. RELX PLC - AFSC Investigate, Zugriff am Februar 14, 2026, https://investigate.afsc.org/company/relx
5. LexisNexis's Contract with ICE as Unjust Enrichment - Colorado Law ..., Zugriff am Februar 14, 2026, https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=1633&context=lawreview
6. GSA and "The Work Number", Zugriff am Februar 14, 2026, https://www.gsa.gov/buy-through-us/purchasing-programs/shared-services/payroll-shared-services/new-employment-verification
7. LOGIN.GOV AND THE UNCERTAIN EARLY LIFE OF AMERICA'S NATIONAL DIGITAL ID - NYU Law Review, Zugriff am Februar 14, 2026, https://nyulawreview.org/wp-content/uploads/2025/04/100-NYU-L-Rev-207.pdf
8. How the Federal Government Buys Our Cell Phone Location Data, Zugriff am Februar 14, 2026, https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data
9. DHS's Data Reservoir | Epic.org, Zugriff am Februar 14, 2026, https://epic.org/wp-content/uploads/2022/08/DHS-Data-Reservoir-Report-Aug2022.pdf

10. ICE Uses a Growing Web of AI Services to Power Its Immigration Enforcement and Surveillance, Zugriff am Februar 14, 2026, https://www.americanimmigrationcouncil.org/blog/ice-uses-ai-immigration-enforcement-surveillance/
11. ICE drives AI use case growth within Homeland Security | FedScoop, Zugriff am Februar 14, 2026, https://fedscoop.com/dhs-ai-inventory-mobile-fortify-palantir/
12. Cook County Board Reapproves Contract with ICE-Linked Data Firm as Raids Sweep Chicago - South Side Weekly, Zugriff am Februar 14, 2026, https://southsideweekly.com/cook-county-board-reapproves-contract-with-ice-linked-data-firm-as-raids-sweep-chicago/
13. The Data Broker to Deportation Pipeline: - Squarespace, Zugriff am Februar 14, 2026, https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/62df020189b0681d1b9398a8/1658782211567/Commercial+and+Utility+Data+Report.pdf
14. A Loophole in the Fourth Amendment: The Government's Unregulated Purchase of Intimate Health Data - UW Law Digital Commons, Zugriff am Februar 14, 2026, https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1076&context=wlro
15. Income & Employment Verification for Government | The Work Number, Zugriff am Februar 14, 2026, https://theworknumber.com/solutions/industries/government-verification
16. American Dragnet | Data-Driven Deportation in the 21st Century, Zugriff am Februar 14, 2026, https://americandragnet.org/
17. AMERICAN DRAGNET, Zugriff am Februar 14, 2026, https://americandragnet.org/sites/default/files/2025-05/American_Dragnet_English_May2025.pdf
18. Commercial data brokers | From Data Criminalization to Prison Abolition, Zugriff am Februar 14, 2026, https://abolishdatacrim.org/en/bestiary/commercial-data-brokers
19. USA/Global: Tech Made by Palantir and Babel Street Pose Surveillance Threats to Pro-Palestine Student Protestors & Migrants - Amnesty International, Zugriff am Februar 14, 2026, https://www.amnestyusa.org/press-releases/usa-global-tech-made-by-palantir-and-babel-street-pose-surveillance-threats-to-pro-palestine-student-protestors-migrants/
20. United States Immigration and Customs Enforcement – AI Use Cases - Homeland Security, Zugriff am Februar 14, 2026, https://www.dhs.gov/ai/use-case-inventory/ice
21. DHS AI Surveillance Arsenal Grows as Agency Defies Courts | TechPolicy.Press, Zugriff am Februar 14, 2026, https://www.techpolicy.press/dhs-ai-surveillance-arsenal-grows-as-agency-defies-courts/

22. Where AI Meets Racism at the Border | TechPolicy.Press, Zugriff am Februar 14, 2026, https://www.techpolicy.press/where-ai-meets-racism-at-the-border/
23. A Start for AI Transparency at DHS with Room to Grow | Brennan Center for Justice, Zugriff am Februar 14, 2026, https://www.brennancenter.org/our-work/analysis-opinion/start-ai-transparency-dhs-room-grow
24. After House Passes Fourth Amendment Is Not For Sale Act, ACLU Urges Senate to Stop Government from Spying on Americans Without a Warrant, Zugriff am Februar 14, 2026, https://www.aclu.org/press-releases/house-passes-fourth-amendment-is-not-for-sale-act
25. H.R.4639 - 118th Congress (2023-2024): Fourth Amendment Is Not For Sale Act, Zugriff am Februar 14, 2026, https://www.congress.gov/bill/118th-congress/house-bill/4639
26. My Votes Explained | Representative Claudia Tenney - House.gov, Zugriff am Februar 14, 2026, https://tenney.house.gov/about/my-votes-explained
27. FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act, Zugriff am Februar 14, 2026, https://www.congress.gov/crs-product/R48592
28. ACLU, EFF Seek to Protect the Public's Right to Access Judicial Records, Zugriff am Februar 14, 2026, https://www.aclu.org/press-releases/aclu-eff-seek-to-protect-the-publics-right-to-access-judicial-records
29. 2026-02-09-the-review-03 - DB Markham, Zugriff am Februar 14, 2026, https://danielbmarkham.com/the-review/2026-02-09-the-review-03