Forensic Data Acquisition and the Erosion of the Private Sphere: A Technical and Legislative Analysis of the Glass Citizen

The concept of the "Glass Citizen" represents the culmination of decades of incremental advancements in data harvesting, predictive analytics, and legislative expansion. It describes a state of existence where the boundary between the private individual and the public record has been effectively dissolved through forensic data acquisition. This phenomenon is not the result of a single technological breakthrough but rather the convergence of six primary "pillars" of surveillance: biological prediction, wearable identity scraping, mandatory age assurance, the paradox of mass data collection, the dismantling of private correspondence, and the commodification of personal data within a shadow market of brokers. This report provides an exhaustive analysis of these pillars, grounded in empirical evidence, legislative text, and technical case studies available as of March 2026.

The Biological Surveillance Pillar: From Predictive Marketing to Criminal Forensics

The transformation of the human body into a readable data set began in the commercial sector, where the ability to predict biological changes offered a profound competitive advantage. This predictive capacity has since migrated into the realm of state forensics, where biological markers are used as evidence in criminal proceedings.

The Genesis of Predictive Modeling: The 2012 Target Paradigm

The foundational case study in biological surveillance is the 2012 revelation of Target Corporation's "pregnancy prediction score".[1] Reporting by Charles Duhigg in the *New York Times* detailed how Target statistician Andrew Pole developed a model to identify expectant mothers before they disclosed their status to friends or family.[1] The business logic was clear: major life transitions, such as pregnancy, create windows of "habit flexibility" where consumer loyalty is most easily captured.[3]

The technical mechanism relied on a "Guest ID" number assigned to every shopper, which linked credit card usage, coupons, and demographic data.[2] Pole identified approximately 25 product categories that, when analyzed in combination, allowed the company to assign a "pregnancy prediction" score and estimate a due date within a small window.[1]

Product Category	Biological/Behavioral Correlation	Trimester Indicator
Unscented Lotion	Sensitivity to odors; skin stretching	Early Second Trimester [1]
Magnesium/Zinc/Calcium	Increased nutritional requirements	First 20 Weeks [1]
Scent-free Soap	Olfactory hypersensitivity	First Trimester [1]
Large Cotton Balls	Sanitation/prenatal care preparation	Late Second Trimester [1]
Hand Sanitizers	Hygiene focus/nesting behaviors	Approaching Due Date [1]
Large Purses/Totes	Substitution for diaper bags	Mid-to-Late Pregnancy [1]
Cocoa Butter	Management of stretch marks	Second Trimester [2]
Washcloths	General infant care preparation	Approaching Due Date [2]

The predictive power of this algorithm was so high that it famously identified the pregnancy of a high-school student before her own father was aware, leading to a public confrontation at a Target store.[1] To mitigate the "creep factor," Target began interspersing baby-related coupons with unrelated items like lawnmowers or lightbulbs to make the targeting feel coincidental.[4] This case established the principle that biological transitions leave a forensic trail in consumer behavior that is highly accurate and difficult to mask.[3]

The Criminalization of "Digital Breadcrumbs" in a Post-Roe Era

Following the 2022 *Dobbs* decision in the United States, the techniques once used for retail marketing were repurposed for the criminalization of reproductive choices. Between 2022 and 2025, search history, location data, and period-tracking app records became central forensic tools in abortion-related prosecutions.[7]

In Nebraska, the case of Jessica and Celeste Burgess (2022-2025) provided a landmark precedent for the use of social media metadata. Authorities served Meta with a warrant for

private Facebook messages, which provided evidence that Jessica Burgess had facilitated her daughter's access to abortion medication.[10] The forensic extraction included between 50 and 250 megabytes of data, encompassing account information and private correspondence.[10]

Evidence Type	Forensic Application in Reproductive Cases	Privacy Risk Level
Period Tracker Logs	Establishing missing cycles as evidence of pregnancy [8]	High (often lacks HIPAA protection)
Search History	Proving "intent" to acquire restricted substances [7]	Extreme (subject to keyword warrants)
Location Data	Identifying visits to clinics or pharmacies [7]	High (often sold by data brokers)
Private Messaging	Direct evidence of planning or assistance [10]	Extreme (accessible via platform warrants)

The legal vulnerability of this data was intensified in June 2025, when a U.S. District Court in Texas (Purl v. HHS) vacated the 2024 HIPAA Privacy Rule meant to protect reproductive health information.[9] The ruling argued that the Biden administration's rule unlawfully preempted state investigative authority.[9] Consequently, as of early 2026, healthcare providers in several states are no longer strictly prohibited from disclosing protected health information (PHI) to law enforcement investigating reproductive health services, even if the care was lawful in the jurisdiction where it was provided.[9] This creates a "surveillance vacuum" where the biological citizen is stripped of medical confidentiality in the face of state forensics.[9]

The Stalker-on-Demand Pillar: Wearables and the Death of Public Anonymity

The second pillar of the Glass Citizen is the decentralization of mass surveillance through AI-enabled wearables. This technological shift allows for the real-time identity scraping of strangers in public spaces, effectively ending the concept of the "anonymous passerby."

Technical Scrutiny: The I-XRAY Project and Meta’s Smart Glasses

In late 2024, security researchers at Harvard demonstrated the "I-XRAY" system, which integrated Meta’s Ray-Ban smart glasses with existing facial recognition APIs to identify strangers in real-time.[15] The system operates through a multi-stage technical pipeline:

1. **Visual Capture:** The smart glasses livestream the user's view to a private digital environment (e.g., a hidden Instagram feed).[15]
2. **Face Recognition Query:** A computer program extract frames and uses facial recognition tools like PimEyes or FaceCheck.id to find URLs linked to the individual.[15]
3. **Data Scraping:** Large Language Models (LLMs) then scrape those URLs to find names, and query public databases like FastPeopleSearch to retrieve home addresses, phone numbers, and family members.[15]
4. **Mobile Delivery:** The stranger's full profile is delivered to the wearer's smartphone within one minute.[15]

The I-XRAY project highlighted that the "privacy LED" included in the glasses—meant to signal when recording is active—is functionally useless in bright or crowded environments.[15] Furthermore, reports in early 2026 revealed that Meta's glasses were recording private moments and sensitive data without user awareness, which were then processed by contractors in Kenya for AI training.[19] These annotators reportedly viewed identifiable images of individuals changing clothes or in intimate situations, proving that "anonymization" claims often fail in technical practice.[20]

Legislative Gaps and the "Household Exemption"

Current UK and EU privacy laws fail to adequately regulate the use of facial recognition by private citizens in public spaces. Under the GDPR, the "household exemption" (Article 2(2)(c)) typically excludes purely personal data processing from the regulation's strict requirements.[21] However, the CJEU's *Rynes* case established that if a surveillance system covers any public space, even partially, the exemption does not apply.[23]

Despite this, there is no effective enforcement mechanism for mobile wearables. The EU AI Act, which enters into full effect in August 2026, prohibits certain "unacceptable risks" (such as social scoring) but does not specifically ban the use of "passive" facial recognition by private individuals using consumer-grade hardware.[24] This creates a scenario where the "Glass Citizen" is subject to constant identity scraping by their peers, with the resulting data often transiting to non-EU countries for processing and training.[19]

Legislative Instrument	**Status as of 2026**	**Privacy Gap for Wearables**
GDPR (EU/UK)	Enforced	"Household exemption" is ambiguous for mobile, public use [21]
EU AI Act	Partial Enforcement (Aug	Focuses on institutional

	2026)	"high-risk" use, not citizen-led scraping [24]
UK Online Safety Act	Enforced (July 2025)	Mandates data collection for age, increasing identification risk [26]
US State Privacy Laws	Variable (e.g., Texas, Colorado)	Prohibit some biometric capture but often exclude private citizens [24]

The Age Assurance Liability Pillar: Mandatory Biometrics and the Risk of Verification

The third pillar of forensic data acquisition is the mandatory verification of age and identity to access digital services. While ostensibly designed for child protection, these systems mandate the collection of sensitive biometric and governmental data, creating permanent digital identities for all users.

The UK Online Safety Act (OSA) and "Highly Effective" Assurance

The UK OSA, which reached a critical enforcement deadline on July 25, 2025, requires platforms to implement "highly effective" age assurance for adult content.[26] Ofcom's guidance specifies that these systems must be technically accurate, robust, and resistant to bypass methods like VPNs.[26]

Third-party vendors like Yoti have become central to this ecosystem. Yoti's facial age estimation software analyzes facial features to predict age without storing images, but it still requires the processing of biometric data.[29] Critics point out that even "zero-data" methods introduce risks, as they necessitate a framework where no citizen can interact with the internet anonymously.[29]

Breach History and the Vulnerability of Identity Vaults

The push for mandatory age verification has created a surge in "Identity Vault" breaches, where the data collected for verification is compromised. Between 2023 and 2025, several high-profile breaches demonstrated the inherent liability of these systems:

- **700Credit (December 2025):** A breach of North America's largest identity verification provider for the automotive sector exposed the records of 5.6 million consumers, including names and Social Security numbers.[33]
- **Discord Age Verification (September 2025):** Hackers accessed Discord's age verification data, including real names, selfies, and government-issued ID documents.[35]
- **Tea Dating App (July 2024):** An unsecured Firebase database exposed 13,000 photo IDs and 59,000 selfies used for user verification.[35]

- **National Public Data (NPD) Breach (August 2024):** A security failure at NPD exposed 2.9 billion records, including the Social Security numbers of nearly every citizen in the US, UK, and Canada.[34]

The centralization of biometric and identity data required by laws like the OSA creates "honeypots" for cybercriminals and state actors.[26] Furthermore, parliamentary debates in the UK in 2026 have highlighted that these requirements often function as a "Trojan Horse" for broader censorship, where the rhetoric of "protecting children" is used to justify the monitoring of all adult discourse.[32]

Breach Event	Date	Impact	Data Compromised
700Credit	Dec 2025	5.6 Million Users	SSNs, Names, Addresses [33]
Discord	Sep 2025	Unknown	Real Names, Selfies, Gov IDs [35]
Chinese Network	Jun 2025	4 Billion Records	WeChat data, Bank details, Home addresses [36]
Conduent	Jan 2025	4.3 Million Users	Personal Information [33]
TransUnion	Aug 2025	4.4 Million Users	SSNs, Dates of Birth [34]

The Data Blindness Paradox: Mass Surveillance vs. Specific Prevention

The fourth pillar examines the "Data Blindness" counter-argument: the theory that the over-collection of data through mass surveillance actually hinders the prevention of specific crimes and terror attacks. This is often described as the "haystack vs. needle" problem.

The "Known to Authorities" Phenomenon

A recurring theme in major European and UK terror attacks is that the perpetrators were already "known to authorities" but were lost in the noise of mass data collection.

- **Manchester Arena Bombing (2017):** The subsequent inquiry revealed that intelligence on the attacker was available but was not prioritized due to the sheer volume of

"low-level" alerts generated by mass surveillance systems.[38]

- **Paris Attacks (2015):** Security experts noted that while the attackers were "known," the ability to track every person with "links to Syria" was impossible due to resource dilution.[39]
- **2023 Bridge Attacks:** Parliamentary critiques suggested that the focus on "general monitoring" of all user content—as proposed in the Online Safety Bill—diverted resources from targeted investigations based on concrete suspicion.[27]

The Critique of "General Monitoring"

Watchdog groups like Big Brother Watch argue that mandatory mass scanning creates a "flood of false and long-known suspicion reports".[40] In Germany, the Federal Criminal Police Office (BKA) reported that 48% of the suspicious activity reports generated by automated scanning were criminally irrelevant.[40] Furthermore, the EU Commission's own reports admitted that leading-edge scanning technology for illicit content has error rates between 13% and 20%.[40]

Surveillance Theory	Objective	Practical Outcome
Targeted Surveillance	Focus on specific suspects with judicial warrants	Higher conviction rates; less collateral damage [40]
Mass Surveillance (Haystack)	Collect all data to find unknown patterns	High false-positive rates; "data blindness" [38]
"Legal but Harmful" Clause	Remove content that causes "serious distress"	Mission creep; censorship of political dissent [32]
Forensic Over-Collection	Mandate age and ID verification for all users	Creation of identity honeypots; erosion of anonymity [26]

The argument for the "Glass Citizen" is often built on the premise that "more data equals more safety." However, the evidence from the last decade suggests that mass data acquisition creates a state of "information overload," where the most critical signals are frequently missed.[38]

The Chat Control Pillar: The Siege of End-to-End Encryption

The fifth pillar is the legislative and technical attempt to dismantle private correspondence through the EU's CSA Regulation, commonly known as "Chat Control." This represents the final

frontier in the forensic acquisition of the citizen's inner life.

The Technical Mechanism of Client-Side Scanning (CSS)

The Chat Control proposal requires communication services (like WhatsApp, Signal, and Telegram) to implement "pre-encryption scanning".[42] Every message or photo would be analyzed against a database of known illicit material *before* the encryption protocol activates.[42] Technical critics, including Matthew Luckie and researchers from Stanford, argue that this creates a "technical architecture" for mass surveillance that can be repurposed for political or social monitoring.[42]

Specific technical criticisms include:

- **Breaking E2EE:** Signal and WhatsApp have stated that CSS is fundamentally incompatible with end-to-end encryption, as it requires a "backdoor" that can be exploited by malicious actors.[42]
- **Context Blindness:** AI models cannot distinguish between "illegal material" and legitimate educational or medical content, leading to the criminalization of innocent users.[40]
- **Identity Mandates:** The regulation encourages mandatory age verification for messengers, ending the possibility of anonymous communication for whistleblowers and journalists.[40]

The March 2026 "Voting Thriller" and the Interim Status

In March 2026, the European Parliament reached a historic impasse on Chat Control. In a "voting thriller" decided by a single vote, the Parliament rejected the automated assessment of private photos as "suspicious".[40] This resulted in the expiration of the "ePrivacy derogation," meaning that US-based companies like Meta and Google must stop the "voluntary" mass scanning of European citizens' private chats.[40]

However, the battle is not over. "Chat Control 2.0" negotiations are continuing, with a focus on mandatory age verification and "risk-based" benchmarks that would force platforms to implement identity checks to avoid being categorized as "high-risk".[40] This demonstrates a persistent legislative "mission creep" toward the total liquification of private correspondence.[37]

The Shadow Market: Data Brokers and the Federated State

The sixth and final pillar of the Glass Citizen is the commodification of the forensic trail within the global data brokerage industry. This pillar explores how private data is consolidated and sold back to state entities, creating a "Federated Data Platform" where the citizen is permanently indexed.

Palantir and the NHS: The Merger of Public Health and State Security

In 2024, the UK NHS awarded a £330 million contract to Palantir Technologies to build the Federated Data Platform (FDP).[44] The FDP is designed to "sit across" NHS Trusts, Integrated Care Boards (ICBs), and NHS England to connect and analyze pre-existing data silos on a national scale.[45]

The specific data silos being merged include:

- **Hospital Bed Availability and Staff Schedules:** For operational optimization.[44]
- **Elective Waiting Lists and Diagnosis Times:** To drive down backlogs.[44]
- **Confidential Patient Information:** Which critics argue could be accessed by the Home Office or police departments via the FDP's "interoperable" architecture.[45]

Charities like Medact have warned that Palantir's software (Foundry) is highly interoperable with its military-focused software (Gotham), allowing for the "drag and drop" of data between health and policing systems.[45] This creates a "UK version of US immigration raids," where patient data is used for state enforcement.[48]

The Global Data Broker Market in 2025/2026

The data broker industry, which aggregates and licenses consumer information, has reached unprecedented scale. By 2025, the global market valuation reached $331.48 billion, with a projected growth to $519.55 billion by 2030.[49]

Metric	2025 Valuation	2030 Forecast	CAGR
Global Data Broker Market	$331.48 Billion [49]	$519.55 Billion [49]	9.3% - 9.6%
Consumer Data Segment	46.03% Share [50]	N/A	High
Healthcare/Life Sciences	Fastest Growth [50]	14.34% CAGR	Very High
Location Data Segment	N/A	13.68% CAGR [50]	High

Major players like Acxiom, Experian, and Epsilon now facilitate the "de-anonymization" of purportedly anonymous datasets.[49] In June 2025, Acxiom partnered with Snowflake to integrate identity resolution directly into cloud environments, allowing brands to link customer

data without "transferring" it, thereby bypassing some traditional privacy hurdles.[51] This "Shadow Market" ensures that every biological, social, and communicative action of the Glass Citizen is recorded, indexed, and available for purchase by both corporate and state actors.[48]

Synthesis: The Forensic Reality of the Glass Citizen

The analysis of these six pillars reveals a cohesive architecture designed to eliminate the possibility of an "off-ledger" life. The biological surveillance of the Target era has evolved into a forensic tool for criminalizing reproductive health.[1] The public anonymity once afforded by the crowd has been destroyed by real-time wearable identity scraping.[15] The digital world is increasingly gated by mandatory biometric age verification, which creates vulnerable identity vaults prone to massive breaches.[29]

Furthermore, the drive for "mass surveillance" has created a state of data blindness, where the over-collection of information prevents the effective identification of real threats.[38] The final sanctuary of private correspondence is under constant siege by "Chat Control" regulations that seek to install a pre-encryption scanning layer in every messaging app.[40] Finally, the data broker industry has successfully merged public and private silos, creating a "Federated Data" environment where the citizen's most sensitive health and location data is a commodified asset.[45]

The "Glass Citizen" is not merely a metaphor for a loss of privacy; it is a technical description of the modern human condition under the regime of total forensic data acquisition. As of March 2026, the indisputable fact is that the infrastructure for a perfectly transparent society is already in place, and the legislative framework to utilize it is expanding with minimal resistance.

Works cited

1. Big Data Insights: Target's Pregnancy Predictions | Yu-kai Chou, accessed March 28, 2026, https://yukaichou.com/chou-musings/big-data-how-target-knows-you-are-pregnant/
2. Using Analytics to Detect Pregnant Shoppers | xraydelta, accessed March 28, 2026, https://xray-delta.com/2012/02/29/using-analytics-to-detect-pregnant-shoppers/
3. The Target Pregnancy Prediction: Analytics Power and Ethics Collide - Othor AI, accessed March 28, 2026, https://blog.othor.ai/the-target-pregnancy-prediction-analytics-power-and-ethics-collide-3177cc7955f7
4. Target Knows You're Pregnant - VICE, accessed March 28, 2026, https://www.vice.com/en/article/target-knows-you-re-pregnant/
5. How Target Used Data Analytics to Predict Pregnancies - Drive Research, accessed March 28, 2026, https://www.driveresearch.com/market-research-company-blog/how-target-used-data-analytics-to-predict-pregnancies/

6. Target: You Can't Hide That Baby Bump From Us - Digital Innovation and Transformation, accessed March 28, 2026, https://d3.harvard.edu/platform-digit/submission/target-you-cant-hide-that-baby-bump-from-us/
7. Stopping the Abuse of Tech in Surveilling and Criminalizing Abortion, accessed March 28, 2026, https://www.americanprogress.org/article/stopping-the-abuse-of-tech-in-surveilling-and-criminalizing-abortion/
8. All Eyes on my Period? Period tracking apps and the future of privacy in a post-Roe world, accessed March 28, 2026, https://privacyinternational.org/long-read/5593/all-eyes-my-period-period-tracking-apps-and-future-privacy-post-roe-world
9. Seventeen States Attack HIPAA and Reproductive Health Privacy | National Partnership for Women & Families, accessed March 28, 2026, https://nationalpartnership.org/report/attacks-on-repro-privacy/
10. From Roe to Risk: The Sobering Realities of Reproductive Data Privacy in a Post-Roe America - DigitalCommons@UM Carey Law, accessed March 28, 2026, https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1457&context=jhclp
11. Understanding Women's Privacy Concerns Toward Period-Tracking Apps in the Post Roe v. Wade Era - Federal Trade Commission, accessed March 28, 2026, https://www.ftc.gov/system/files/ftc_gov/pdf/10-Laabadli-Understanding-Womens-Privacy-Concerns-Toward-Period-Tracking-Apps-in-the-Post-Roe-v-Wade-Era.pdf
12. Healthcare Law Alert: Federal Court Ruling Vacates HIPAA Privacy Rule to Support Reproductive Health Care Privacy - Hancock Estabrook, LLP, accessed March 28, 2026, https://www.hancocklaw.com/publications/healthcare-law-alert-federal-court-ruling-vacates-hipaa-privacy-rule-to-support-reproductive-health-care-privacy/
13. Court Vacates 2024 Reproductive Health Care Rule - Keenan, accessed March 28, 2026, https://www.keenan.com/knowledge-center/news-and-insights/briefings/court-vacates-2024-reproductive-health-care-rule/
14. HIPAA and Reproductive Health | HHS.gov, accessed March 28, 2026, https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/index.html
15. PRIVACY AT RISK: HARVARD STUDENTS EXPOSES DARK SIDE OF META'S SMART GLASSES - JustAI, accessed March 28, 2026, https://justai.in/privacy-at-risk-harvard-students-exposes-dark-side-of-metas-smart-glasses/
16. Harvard students adapt Meta smart glasses to reveal people's ... - ITVX, accessed March 28, 2026, https://www.itv.com/news/2024-10-05/harvard-students-use-metas-smart-glasses-to-create-a-privacy-nightmare
17. Smart glasses raise privacy concerns, Harvard students show in study - YouTube,

accessed March 28, 2026, https://www.youtube.com/watch?v=aqrolPymsFw
18. The Dark Side of Meta's Smart Glasses: How I-XRAY Exposes a Disturbing Reality, accessed March 28, 2026, https://twit.tv/posts/tech/dark-side-metas-smart-glasses-how-i-xray-exposes-disturbing-reality
19. Parliamentary question | Privacy risks and GDPR compliance issues ..., accessed March 28, 2026, https://www.europarl.europa.eu/doceo/document/P-10-2026-000903_EN.html
20. Meta withholds Display Glasses from the EU: Should Smartglasses Be Exempt from New Battery Rules? : r/augmentedreality - Reddit, accessed March 28, 2026, https://www.reddit.com/r/augmentedreality/comments/1s315ds/meta_withholds_display_glasses_from_the_eu_should/
21. Full article: The data-driven home: towards a more coherent regulatory framework for smart homes in the European Union - Taylor & Francis, accessed March 28, 2026, https://www.tandfonline.com/doi/full/10.1080/13600834.2025.2572918
22. Interdependent Privacy in Smart Homes: Hunting for Bystanders in Privacy Policies - arXiv, accessed March 28, 2026, https://arxiv.org/html/2510.26523v1
23. When Privacy and Security Collide: the legality of using facial recognition security systems in quasi-public spaces – Raghav Mendiratta - Inforrm's Blog, accessed March 28, 2026, https://inforrm.org/2020/06/05/when-privacy-and-security-collide-the-legality-of-using-facial-recognition-security-systems-in-quasi-public-spaces-raghav-mendiratta/
24. Global Privacy Watchlist | Insights - Mayer Brown, accessed March 28, 2026, https://www.mayerbrown.com/en/insights/publications/2026/01/global-privacy-watchlist
25. EU AI Act 2026 Updates: Compliance Requirements and Business Risks - Legal Nodes, accessed March 28, 2026, https://www.legalnodes.com/article/eu-ai-act-2026-updates-compliance-requirements-and-business-risks
26. You Must Be This Tall to Click: The Online Safety Act and Age-Appropriate Access - Katten, accessed March 28, 2026, https://quickreads.ext.katten.com/post/102ku9h/you-must-be-this-tall-to-click-the-online-safety-act-and-age-appropriate-access
27. The UK Online Safety Bill: A Massive Threat to Online Privacy, Security, and Speech, accessed March 28, 2026, https://www.eff.org/pages/uk-online-safety-bill-massive-threat-online-privacy-security-and-speech
28. Privacy Advocates Urge Regulators to Block Meta's Facial Recognition Smart Glasses Plan, accessed March 28, 2026, https://babl.ai/privacy-advocates-urge-regulators-to-block-metas-facial-recognition-smart-glasses-plan/
29. Age Assurance Technologies and Online Safety, accessed March 28, 2026, https://cetas.turing.ac.uk/publications/age-assurance-technologies-and-online-sa

fety
30. Ofcom and ICO Issue Joint Statement on Age Assurance - Inside Privacy, accessed March 28, 2026, https://www.insideprivacy.com/online-safety/ofcom-and-ico-issue-joint-statement-on-age-assurance/
31. Age assurance: the facts - Yoti, accessed March 28, 2026, https://www.yoti.com/blog/age-assurance-the-facts/
32. The Online Safety Act Has Nothing to Do With Child Safety and Everything to Do With Censorship | Kate Sim | Novara Media, accessed March 28, 2026, https://novaramedia.com/2025/08/07/the-online-safety-act-has-nothing-to-do-with-child-safety-and-everything-to-do-with-censorship/
33. Data Breaches That Have Happened This Year (2026 Update) - Tech.co, accessed March 28, 2026, https://tech.co/news/data-breaches-updated-list
34. DATCP Home Data Breaches - Wisconsin.gov, accessed March 28, 2026, https://datcp.wi.gov/pages/programs_services/databreaches.aspx
35. The Breachies 2025: The Worst, Weirdest, Most Impactful Data Breaches of the Year, accessed March 28, 2026, https://www.eff.org/deeplinks/2025/12/breachies-2025-worst-weirdest-most-impactful-data-breaches-year
36. 27 Biggest Data Breaches Globally (+ Lessons) 2025 - Huntress, accessed March 28, 2026, https://www.huntress.com/blog/biggest-data-breaches
37. Online Safety Act: Privacy Threats and Free Speech Risks - The Constitution Society, accessed March 28, 2026, https://consoc.org.uk/the-online-safety-act-privacy-threats-and-free-speech-risks/
38. 'Either a sell-out or an extremist': - Examining the experiences of Muslim and minority ethnic practitioners implementing Prevent and the Counter-Extremism Strategy in Birmingham SAMIA YASMIN, accessed March 28, 2026, https://publications.aston.ac.uk/id/eprint/47851/1/YASMIN_SAMIA_2023.pdf
39. November 2015 Paris attacks - Wikipedia, accessed March 28, 2026, https://en.wikipedia.org/wiki/November_2015_Paris_attacks
40. End of “Chat Control”: EU Parliament Stops Mass Surveillance in ..., accessed March 28, 2026, https://www.patrick-breyer.de/en/end-of-chat-control-eu-parliament-stops-mass-surveillance-in-voting-thriller-paving-the-way-for-genuine-child-protection/
41. Chat Control is in the final stretch - European Digital Rights (EDRi), accessed March 28, 2026, https://edri.org/our-work/chat-control-is-in-the-final-stretch-but-it-could-be-a-marathon-not-a-sprint/
42. How Europe's “Chat Control” Regulation Could Compromise American Communications, accessed March 28, 2026, https://www.techpolicy.press/how-europes-chat-control-regulation-could-compromise-american-communications/
43. After Years of Controversy, the EU's Chat Control Nears Its Final Hurdle: What to Know, accessed March 28, 2026,

https://www.eff.org/deeplinks/2025/12/after-years-controversy-eus-chat-control-nears-its-final-hurdle-what-know
44. NHS to begin roll-out of federated data platform in spring 2024 - Hospital Times, accessed March 28, 2026, https://hospitaltimes.co.uk/nhs-begin-roll-out-federated-data-platform-spring-2024/
45. Briefing: Concerns Regarding Palantir Technologies and NHS Data ..., accessed March 28, 2026, https://www.medact.org/2026/resources/briefings/briefing-palantir-fdp/
46. New strategic collaboration aims to upskill staff on the NHS Federated Data Platform - Palantir IR - News, accessed March 28, 2026, https://investors.palantir.com/news-details/2025/Multiverse-and-Palantir-Partner-to-Launch-NHS-Federated-Data-Platform-Apprenticeship-Programmes-Supporting-the-NHSs-Data-and-AI-Transformation/
47. UK Healthcare - Palantir, accessed March 28, 2026, https://www.palantir.com/uk/healthcare/
48. Palantir's NHS England contract 'opens door to government abuse of power', health bosses told - The Guardian, accessed March 28, 2026, https://www.theguardian.com/technology/2026/mar/12/palantirs-nhs-england-contract-opens-door-to-government-abuse-of-power-health-bosses-told
49. Data Broker Market Global Trends, Scope Report 2026 - The Business Research Company, accessed March 28, 2026, https://www.thebusinessresearchcompany.com/report/data-broker-global-market-report
50. Data Broker Market Size, Growth, Trends & Forecast Report 2031 - Mordor Intelligence, accessed March 28, 2026, https://www.mordorintelligence.com/industry-reports/data-broker-market
51. Data Broker Market Size and Outlook 2031 - TechSci Research, accessed March 28, 2026, https://www.techsciresearch.com/report/data-broker-market/18734.html
52. Global Data Broker Market Predicted to Reach US$616.541 Billion by 2030, accessed March 28, 2026, https://www.globenewswire.com/news-release/2025/02/14/3026669/0/en/Global-Data-Broker-Market-Predicted-to-Reach-US-616-541-Billion-by-2030.html