STUDY

# Data bought, rights ignored: European intelligence services' use of commercially sourced data

Corbinian Ruckerbauer, Thorsten Wetzling

June 16, 2026

Tech analysis and policy ideas for Europe

interface

# Table of Contents

# 1. Executive summary

Personal data generated through everyday app and platform use has become a tradable commodity that European governments increasingly purchase and exploit for national security, law enforcement, and defence purposes. While procurement practices differ, the scale and scope of this private–public co-production of intelligence based on commercially sourced data should be of far greater concern to European regulators, oversight bodies, and the public.

Investigative reporting by Netzpolitik.org and Bayerischer Rundfunk showed how easily 3.6 billion location data points, covering millions of individuals, including military personnel, intelligence staff, and senior government officials, can be purchased. The Citizen Lab documented widespread *government* use of Webloc, a private-sector geolocation analysis tool harvesting data from the mobile advertising ecosystem. Journalists also found Hungarian intelligence services using it, and it is unlikely that other EU Member States abstain from similar practices.

Government use of commercially sourced data can seriously interfere with fundamental rights, including the right to privacy and informational self-determination. It also creates national security risks: close cooperation with private firms and reliance on vast datasets may expose agencies, personnel, and critical infrastructure to exploitation by hostile actors.

Despite growing media attention to advertisement-based intelligence (ADINT), European parliaments are only beginning to grapple with the implications of this mode of intelligence production. Key questions are: do national legal frameworks adequately regulate the acquisition and use of commercially sourced data, and are oversight bodies sufficiently equipped to ensure accountability? To learn more about this, we surveyed intelligence oversight practitioners from eleven democracies. The findings are concerning:

- Several oversight practitioners reported that they cannot review, reshape or prevent government contracts with data brokers and other private sector entities;
- All but one delegation in our sample said they are not informed when new contracts are concluded, and no delegation has a binding power to delay or block such contracts;
- Most practitioners said their oversight institutions cannot publicly report on the scope of intelligence access to commercially sourced data;
- Although inspections and audits of data-sharing with domestic and foreign partners fall within most oversight bodies' mandates, no delegation reported that they had carried out an inspection or audit on the topic of data transfers involving commercially sourced data.

A comparative review of intelligence laws in the Netherlands, the United Kingdom, the United States, and Germany further reveals significant legal gaps and ambiguities. None of these jurisdictions provides a coherent statutory framework governing the full lifecycle of commercially sourced data, from acquisition and access to processing, sharing, deletion, and reporting, demonstrating just how regulation lags behind operational practice.

We thus call for urgent reforms and less credulous oversight. Regulators should

- include **new warrant requirements** applicable to commercially sourced data so that intelligence agencies can no longer avoid the rules and safeguards that would otherwise apply to their use of bulk personal data;
- address **the procurement of commercially sourced data prior to the conclusion of contracts with private sector entities**, particularly in cases involving the testing of new technologies in cooperation with private companies;
- create a **legal basis for mediated data use**, e.g. when intelligence agencies access and use data stored on the servers of private sector entities;
- require a mandatory **inventory of databases** not just for those that the intelligence agencies use on their own IT systems but also for those to which they have mediated access;
- grant **full access to oversight bodies** to all data storage locations, documentations and information systems;
- require that **comprehensive log recordings** must be made available to oversight bodies for the purpose of their audits;
- define when and how commercially sourced data can be **shared** with other agencies and third parties so as mitigate the risk of circumventing rules on purpose limitation;
- empower oversight bodies to **compel private sector entities** to provide information deemed necessary for their investigations and audits.

Oversight bodies should

- **reach out more proactively to national data protection authorities** overseeing the processing of data in the private sector and identify ways in which they could potentially help each other;
- see if **a responsible use of AI tools**, e.g. to review contracts between intelligence services and private actors prior to their conclusion, can help compensate scarce resources without adding new risks and concerns;
- regularly **review log recordings** and demand more granular information from the services if necessary;
- regularly **assess the purposes for which commercially sourced data is being used;**
- **report** on the practice of data purchases to the maximum extend that they legally can.

Comprehensive regulation and effective oversight of agencies' use of commercially sourced data do not require a trade-off between security and fundamental rights. Yet, unconstrained use of advertising-based intelligence undermines both. The same datasets used by European agencies are also accessible to foreign adversaries, who are already exploiting them. More regulation of commercially sourced data, combined with robust oversight, is not a constraint on intelligence work but a precondition for secure, lawful,

and legitimate operations. It is also a foreign policy imperative: only genuine efforts at intelligence accountability allow our democracies to credibly repudiate unconstrained electronic surveillance by authoritarian regimes.

---

*Acknowledgements:* We thank Svenja Efinger for excellent background research and factchecking. Our former colleague, Lilly Goll, also contributed significantly to this work. Luisa Seeling and Alina Siebert have provided excellent editorial and graphic design support and we thank them also for having accommodated shifting deadlines. The authors are solely responsible for any factual errors.

---

# 2. Introduction

*OpenAI's systems "shall not be intentionally used for domestic surveillance of U.S. persons and nationals [...] including through the procurement or use of commercially acquired personal or identifiable information".*[1]

National security agencies cooperate very closely with technology companies and data brokers to acquire, access, and use large volumes of personal data held by the private sector. Much of this cooperation is voluntary in nature.[2] It is also big business:[3] Intelligence and security agencies are now spending millions of taxpayers' money on what some call *ad-based surveillance technology services*.[4] Not just in the United States but also in the European Union.[5]

Policymakers and regulators need to know much more about the different forms of private-public co-production of intelligence that are commonly known as *advertising-based intelligence* (ADINT).[6] They have profound implications for the democracies they serve. They interfere with fundamental rights and cause risks to

---

1 Cade Metz and Julian E. Barnes, *OpenAI Amends A.I. Deal With the Pentagon* (2026), https://www.nytimes.com/2026/03/02/technology/openai-pentagon-deal-amended-surveillance.html. (our emphasis)

2 This is markedly different from *compelled government access to data* where, for example, a government serves an internet service provider a *technical capability notice* to legally oblige them to render access to their IT systems.

3 Brennan Center et al., *Joint Comment Regarding OMB's Request for Information on Executive Branch Agency Handling of Commercially Available Information* (2024), https://epic.org/documents/join-comment-regarding-ombs-request-for-information-on-executive-branch-agency-handling-of-commercially-available-information/, pp. 14-15.

4 For a recent and very insightful documentation of this, see: Wolfie Christl et al., *Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech* (2026), Citizen Lab Report, https://citizenlab.ca/research/analysis-of-penlinks-ad-based-geolocation-surveillance-tech/.

5 Szabolcs Panyi, *Orbán's Spying Kit Revealed: Israeli Surveillance Tool Combined with Hungarian Technology* (2026), https://vsquare.org/orban-spying-toolkit-cobwebs-webloc-hungary-spyware-citizen-lab/; Martin Untersinger, *How surveillance companies track smartphone users through advertising data* (22 January 2026), https://www.lemonde.fr/en/pixels/article/2026/01/22/how-surveillance-companies-track-smartphone-users-through-advertising-data_6749674_13.html.

6 Paul Vines, Franziska Roesner, and Tadayoshi Kohno, *Exploring ADINT: Using Ad Targeting for Surveillance on a Budget - or - How Alice can Buy Ads to Track Bob* (2017), adint.cs.washington.edu/ADINT.pdf.

national security, too. Do national legal frameworks for intelligence sufficiently regulate the agencies' acquisition and use of commercially sourced data? Are national oversight and accountability mechanisms fit for purpose when it comes to national intelligence agencies' involvement in ADINT?

This report seeks to provide answers to these important and consequential questions. Before it can meaningfully do so, it ought to provide further context on the data market, possible scenarios for intelligence services' procurement and use of commercially sourced data as well as reported instances of such practices.

## 2.1. The data market and procurement trajectories

The commercial data market provides very granular information on virtually every individual to its various clients. Vendors sell enormous datasets of highly sensitive information related to individuals' location, age, gender, political preferences, interests, sexual orientation, religious beliefs, and communication patterns.

Both the sources of such data and their procurement trajectories are diverse and opaque. The data can, for example, stem from real-time bidding (RTB) auctions[7] and software development kits (SDK)[8] to social media platforms, the exploitation of technical vulnerabilities,[9] and applications connected to the internet-of-things (IoT). Many of these processes are primarily designed to enable targeted advertising, product optimisation, and enhanced user experiences. The data generated in such processes has become a hugely attractive economic commodity. Companies systematically collect, aggregate, and analyse this information to monetise their services.

Because these datasets contain an enormous amount of information about individuals, they are also of core interest to intelligence and security agencies. They acquire it by means of different procurement trajectories as illustrated below. The following list is not meant to be exhaustive.

***Direct procurement of commercially sourced data***

One way for intelligence agencies to acquire such data is through a direct purchase from commercial vendors. This can be single data points or – more likely, whole datasets, that oftentimes have been generated from data collections supposed to be useful for advertising or consumer profiling. In other cases, data can stem from illegal data leaks.

7 Lena Cohen, *Online Behavioral Ads Fuel the Surveillance Industry—Here's How* (2025), https://www.eff.org/deeplinks/2025/01/online-behavioral-ads-fuel-surveillance-industry-heres-how.

8 Bennett Cyphers, *How the Federal Government Buys Our Cell Phone Location Data* (2022), https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data.

9 Lighthouse Reports, *How First Wap Tracks Phones Around the World* (2025), https://www.lighthousereports.com/methodology/surveillance-secrets-explainer/.

For example, in 2024 the Dutch intelligence oversight body CTIVD reported that the Dutch intelligence services acquired multiple bulk datasets mostly consisting of "tens of millions of data" and mostly originating "from the internal systems of companies and institutions" for national security purposes.[10] In other cases, data collections can be designed from the outset to be useful for security services.[11]

***Platform-based access via commercial analytics tools***

Rather than acquiring raw datasets, agencies can also rely on integrated platforms that provide access to aggregated and processed data and combine different types and sources. One example for this type of platforms is the platform Tangles developed by the Israeli-U.S company Penlink that is used by several public authorities. The software enables the analysis of social media and dark web activity.[12]

***Refinement of internal databases and training AI models***

Commercially sourced data may be used to enrich already existing internal databases, that were established with the help of traditional data collection methods. Furthermore, commercially sourced data can be used to train AI-models.[13]

See for example the review report on the UK Investigatory Powers Act:

*"best data on which to train models tend to be open source, publicly available and sometimes commercially curated. When building models, intelligence services are not interrogating the data to identify individual records of intelligence interest, but are using the structure and attributes of the whole dataset to build capability and tools to help deliver their intelligence functions. This activity is likely to continue, and to grow, in the future."*[14]

In other words, intelligence services are not using this data to investigate specific individuals, but rather to build broader analytical capabilities.

***Hybrid public-private development***

Agencies may also combine external procurement with internal development to replicate or enhance commercial capabilities. Reporting indicates that this is what the Hungarian intelligence community tried to do. While using a private sector "geolocation surveillance

10 CTIVD, *Toezichtsrapport nr 79 over de inzet van virtuele agenten door de AIVD en de MIVD* (2024), p. 14, https://www.ctivd.nl/documenten/rapporten/2024/09/09/index.

11 Lighthouse Reports, *How First Wap Tracks Phones Around the World* (2026), https://www.lighthousereports.com/methodology/surveillance-secrets-explainer/.

12 Wolfie Christl et al., *Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech.*

13 Cade Metz and Julian E. Barnes, *OpenAI Amends A.I. Deal With the Pentagon* (2026), https://www.nytimes.com/2026/03/02/technology/openai-pentagon-deal-amended-surveillance.html.

14 David Anderson, *Independent Review of the Investigatory Powers Act 2016* (2024), https://www.ssrn.com/abstract=4833577.

system called Webloc" which "uses ad-based data to monitor hundreds of millions of people across the globe"[15], they simultaneously explored building a domestic system with similar functionality according to recent reporting.[16]

***Direct collection***

Intelligence agencies may as well use shell companies to directly engage in the ad tech industry and collect data. Since the threshold to, for example, register for demand-side platforms to extract information from RTB-procedures is relatively low, this may be an uncomplicated way to access this type of geolocation data.

In sum, personal data is being traded within a rapidly expanding commercial ecosystem that is incredibly complex and difficult to scrutinise. The scale, opacity, and fragmentation of the data market pose significant challenges for transparency, accountability, and regulatory oversight – all of which is becoming even more obscure when the clients are national intelligence services.

## 2.2. Exhibits of widespread ADINT

A growing number of signs point to direct intelligence service activity on the data market. In some cases, evidence of data purchases is publicly available. The following section draws attention to a few selected instances from jurisdictions in Europea and North America. The list would be much longer, obviously, if it also featured instances of authoritarian governments' use of advertising-based technology and commercially sourced data.[17]

**Hungarian Intelligence Community:** According to research by the Central European investigative journalism platform VSquare and the Canadian Citizen Lab, at least three Hungarian intelligence services have been using Penlink's Webloc tool since 2022.[18] When these findings were published in April 2026, they offered the first proof for the systematic use of geolocation data from the data industry by security agencies in an EU Member State. Besides purchasing a license to use this foreign software solution, VSquare also reported that the Hungarian services were aiming to build their own technical solution that offered similar capabilities.

---

15 Wolfie Christl et al., *Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech.*

16 Szabolcs Panyi, *Orbán's Spying Kit Revealed: Israeli Surveillance Tool Combined with Hungarian Technology*.

17 For information on ADINT as a method used in digital transnational repression, see: Siena Anstis, Tristan Surman, Noura Aljizawi, Marcus Michaelsen and Ron Deibert, *Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the Committee on Enforced Disappearances and the Working Group on Enforced or Involuntary Disappearances* (2026), https://citizenlab.ca/wp-content/uploads/2026/02/Submission_The-Citizen-Lab_30-January-2026_Call-for-inputs-on-Enforced-Disappearances-in-the-context-of-transnational-repression.pdf

18 This product is provided by Israeli company Cobwebs Technology that has been purchased by the US company Penlink. It is part of the *Tangles* platform, combining multiple tools for monitoring activities in the open web, deep web and darkweb – including capabilities for image and facial recognition as well as natural language processing. It is furthermore able to analyse patterns and connect target individuals to other contacts and events. See Szabolcs Panyi, *Orbán's Spying Kit Revealed: Israeli Surveillance Tool Combined with Hungarian Technology*.

**U.S. Federal Bureau of Investigation**: In 2023, then FBI Director Christopher Wray testified that the FBI was not, at that time, purchasing location data derived from internet advertising, while acknowledging that it had done so previously for a national security pilot project. He added that since then the FBI was using a court-authorised process to obtain such data.[19] In 2025, the U.S. Privacy and Civil Liberties Oversight Board (PCLOB) released an unclassified staff report of its investigation into the FBI's use of Open Source Information. According to the staff report, "PCLOB's review confirmed the FBI does not purchase real time continuous location information, one of the most sensitive types of data."[20] The report stated, however, that the FBI uses commercial services and tools to access open source information. It also pointed out that "commercial tools consolidate substantial amounts of open source information, enabling users to more efficiently conduct searches by bypassing the need to visit individual websites and conduct manual searches" and that "the FBI reported that its employees may directly access and enter search terms into commercial tools."[21] PCLOB's staff report described several of those tools and the policy limitations on use. Information on the use of tools such as Clearview AI, ZeroFox and Babel Street were not included, however.

**U.S. Customs and Border Protection (CBP):** Reporting by *404 Media* in 2026 featured an internal Privacy Threshold Analysis produced by the CBP.[22] In this document the institution laid out details on a pilot named "AdID Efficacy Pilot" running from 2019 to 2021.[23] Within this analysis, CBP acknowledged acquiring personal information both directly from a data broker and indirectly via two commercial platforms. The data in question included location information derived from Software Development Kits (SDKs) and Real-Time Bidding (RTB) streams.

**U.S. Immigration and Customs Enforcement (ICE) and Homeland Security Investigation (HIS):** These agencies, both entities of the Department of Homeland Security (DHS), issued a request for information seeking private-sector capabilities in big data and advertising technology, with the aim of further integrating such resources into their operations. The document invited providers to specify the types of data they could supply on various targets, including individuals. This request has been interpreted as an indication of a continued or expanded reliance on commercially sourced sensitive data.[24]

19 Dell Cameron, *The FBI Just Admitted It Bought US Location Data* (2023), https://www.wired.com/story/fbi-purchase-location-data-wray-senate/.

20 PCLOB Staff Report, *Use of Open Source Information by the Federal Bureau of Investigation* (2026), https://documents.pclob.gov/prod/DynamicImages/Generic/fd7d5577-e5c9-4247-ade7-b71e5937e41e/%28U%29%20Use%20of%20Open%20Source%20Information%20by%20the%20FBI.pdf

21 Ibid.

22 Joseph Cox, *CBP Tapped Into the Online Advertising Ecosystem To Track Peoples' Movements* (2026), https://www.404media.co/cbp-tapped-into-the-online-advertising-ecosystem-to-track-peoples-movements/.

23 Privacy Office U.S. Department of Homeland Security, *Privacy Threshold Analysis - AdID Efficacy Pilot* (2022), https://www.documentcloud.org/documents/27714350-adid-efficacy-pilot-pta/.

In 2023 the DHS released an internal report stating that several DHS entities, including ICE, violated "federal law through their purchases of 'commercial telemetry data (CTD) collected from mobile devices that included, among other things historical device location'".[25]

**Austrian Ministry of the Interior:** The Ministry is on the record for having procured Penlink's surveillance tool *Tangles*.[26] As reported in April 2026, a Tangles plug-in known as *Webloc* allows for the analysis of location data derived from the advertising technology ecosystem. The Austrian government declined to clarify whether this functionality is operational within Austrian law enforcement or to what extent it is being used, despite inquiries from researchers and political opposition.

**French intelligence service Direction générale de la Sécurité extérieure (DGSE):** In 2021, the DGSE requested that the French legislature establish a legal basis permitting it to purchase internet browsing data from private companies. No such explicit legal authorisation has been enacted to date yet. However, the absence of a formal legal framework does not necessarily preclude the practice. On the contrary, the agency's earlier articulation of an operational need may suggest that alternative avenues for accessing such data have been tested in pilot projects.[27]

**Norwegian Intelligence Service (NIS):** The Norwegian oversight body (EOS Committee) has reported on multiple occasions that the NIS had been "purchasing metadata from commercial enterprises".[28] While the oversight body has not specified the companies or datasets involved, it has criticized the lack of a clear legal basis, concluding that the practice is unlawful under current regulations. Following repeated scrutiny and recommendations, the Norwegian Ministry of Defence indicated that it now applies the same procedural rules to such acquisitions as it does to the collection of openly available information.[29]

**Dutch Intelligence Community:** The Dutch oversight body CTIVD published reports on the use of commercially acquired data by the Dutch intelligence community in 2018 and 2024. The analysis over time shows a marked increase in the reliance on information purchased from private entities. The CTIVD highlights shortcomings in the application of the current legal framework for data purchases in both reports. In March 2025, the Dutch

24 Sheera Frenkel and Aaron Krolik, *How ICE Already Knows Who Minneapolis Protesters Are*, (2026), https://www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html.

25 Wolfie Christl et al., *Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech.*

26 Andreas Proschofsky, *Innenministerium nutzt Überwachungssoftware von zwielichtiger Firma, will nicht darüber reden* (2026), https://www.derstandard.at/story/3000000309258/innenministerium-nutzt-ueberwachungssoftware-von-zwielichtiger-firma-will-nicht-darueber-reden.

27 Pierre Gastineau, *Loi de Programmation Militaire : Le Cahier de Doléances de La DGSE* (2022), https://www.intelligenceonline.fr/europe-russie/2022/07/04/loi-de-programmation-militaire--le-cahier-de-doleances-de-la-dgse,109796352-eve.

28 EOS-Committee, *Annual Report 2022* (2023), https://eos-utvalget.no/wp-content/uploads/2023/06/EOS-Committee-annual-report-2022.pdf.

29 EOS-Committee, *EOS Annual Report 2024* (2025), https://eos-utvalget.no/wp-content/uploads/2025/06/EOS-annual-report-2024.pdf.

government announced improvements regarding the application of the correct legal basis as well as the implementation of refined data processing practices.[30] For the upcoming reform CTIVD recommends establishing a more foreseeable legal basis.

**Webloc training session on the premises of the local police in Venice, Italy**. The Citizenlab report on Webloc also features a social media post with a photo from a "Tangles and Webloc Learning by Doing" training session. It was supposedly held at the premises of the local police in Venice from 04 to 06 July 2022.[31]

These examples point to a momentous shift towards the exploitation of commercially sourced data in modern intelligence practice. As the next section shows, this comes with a great number of risks.

## 2.3. Risks

The acquisition of commercially available datasets, along with other forms of cooperation with private sector entities, presents intelligence services with a dilemma: On the one hand, the use of such data sources may enhance operational capabilities. On the other hand, it introduces significant risks affecting both national security and the protection of fundamental rights.

### Fundamental rights and democratic control

The inherently secretive nature of intelligence work means that discriminatory, disproportionate, or unlawful practices may remain unnoticed and, by extension, unchallenged. It is, therefore, essential to ensure that independent oversight bodies are equipped with sufficient capabilities, competences, access, and resources to hold the national security sector to account.

The ongoing paradigm shift in intelligence practice poses significant challenges to the attainment of these preconditions for effective oversight, however.

***Interferences with fundamental rights***

The extensive scope and granularity of data potentially available to security authorities significantly amplifies the impact on individuals whose fundamental rights may be affected. This concerns the right to privacy and informational self-determination, as well as the freedoms of the press, expression, and assembly to name just a few examples.

30 Dutch Government, *Toezegging over de Opvolging van Aanbevelingen in Toezichtrapport 79 over de Inzet van Virtuele Agenten door de AIVD en de MIVD* (2025). Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2025/03/11/kamerbrief-toezegging-over-de-opvolging-van-aanbevelingen-in-toezichtrapport-79-over-de-inzet-van-virtuele-agenten-door-de-aivd-en-de-mivd

31 Wolfie Christl et al., *Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech*.

Particularly at risk are minority groups, such as ethnic, religious, or political groups. Migrants and asylum seekers, for example, were in the recent past among the first ones affected by new forms of surveillance. In addition, journalists and other media professionals, may be compromised in their ability to protect sources. Political activists and members of social movements may face chilling effects when exercising their rights to free expression and assembly. So can civil society organisations that engage in advocacy campaigns.

While the processing of large-scale datasets does not target specific individuals, the dispersed and wide-ranging nature of rights' interferences affect a very large number people. It raises serious questions regarding the application of proportionality principles, which traditionally rely on more clearly defined and targeted measures. The integration of these large-scale, often untargeted data collection practices with advanced analytical tools, including artificial intelligence, further intensifies the pressure on fundamental rights. The ability to derive sensitive insights, predict behaviour, and establish patterns from seemingly innocuous data significantly increases both the depth and the opacity of state interference.

**Mission creep** further exacerbates these concerns. Tools and systems initially justified for specific, high-stakes purposes, e.g. counterterrorism, the fight against sex trafficking or border security, often expand in scope to encompass a much broader range of applications. For example, surveillance technologies purchased for targeted investigations into counterterrorism may be repurposed for routine law enforcement investigations into minor offenses, or even the monitoring of political protests. This gradual shift not only undermines the original justification for such intrusive measures but also normalises their use across unrelated contexts, eroding public trust and the proportionality of state interference.[32]

### *Sizeable and dangerous loopholes in national legal frameworks*

While the inherent tension between secret intelligence collection for open societies is not new, the current developments introduce qualitatively different challenges to fundamental rights. Over the past fifteen years, driven in part by Edward Snowden's revelations of mass surveillance and evolving jurisprudence at both national and international levels, many democratic states have adjusted and reformed their legal frameworks on government surveillance, particularly the sections governing the interception of communications data.

32 Wolfie Christl et al., *Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech;* Jerod MacDonald-Evoy, *Tucson PD Used Border Security Money for Controversial Surveillance Software* (2025), https://azmirror.com/2025/10/29/tpd-used-border-security-money-for-controversial-surveillance-software/.

However, the various forms of interactions between intelligence services and private sector entities largely fall outside these established regulatory regimes. As a result, data access and analysis are likely to occur without the regulatory safeguards and oversight mechanisms that are standard for comparable forms of government surveillance. This accountability gap creates problematic incentives for security agencies to circumvent stricter legal constraints by relying on alternative channels of data acquisition and data handling. It also means that intelligence services may gain access to information that they would not have been permitted to collect under traditional legal standards.

Such gaps also undermine the coherence of the entire legal framework which is supposed to guarantee the rule of law. They also risk eroding public trust in the legitimacy of security agencies' activities.

***Ineffective accountability and redress mechanisms***

Where data processing takes place in opaque environments, particularly on the servers of private companies, individuals often lack realistic means of determining whether they have been subject to surveillance or data analysis practices. Even where individuals develop reasonable suspicion and seek clarification through legally established channels, such as independent oversight authorities, these bodies may themselves be unable to fully assess the extent to which the individual's data has been collected and processed. Legal safeguards such as independent *ex ante* authorisation and *ex post* notification obligations that exist for other forms of data collection may not yet apply.

Furthermore, the intertwining activities of private actors and public authorities may lead to a diffusion of responsibility. It may be particularly complicated to hold specific actors accountable when public and privately held data are fused and subsequently processed with complex data analysis tools. The increasing asymmetry of technological capabilities between intelligence services on the one hand and oversight bodies on the other only add to the challenge.

***Financial support for actors fuelling transnational repression***

Nefarious actors surely exist on the opaque data market. National intelligence services that purchase data from them may inadvertently support transnational digital repression. In fact, they may be financing actors that directly undermine the very protections that their own governments seek to provide to vulnerable individuals. This particularly affects journalists, activists and political dissidents. The proliferation of commercially sourced data, traded for profit, creates an ideal environment for authoritarian regimes, too. These regimes exploit such data to intimidate, persecute or physically and psychologically harm individuals deemed undesirable, even beyond the reach of their formal state authority.[33]

33 Siena Anstis et al., *Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the Committee on Enforced Disappearances and the Working Group on Enforced or Involuntary Disappearances*.

## National security risks

Beyond the above-mentioned risks to individual fundamental rights, the rule of law and democracy, there are also significant national security risks stemming from the private-public co-production of intelligence based on commercially sourced information. While such cooperation may enhance operational capabilities, it also introduces structural vulnerabilities. Close cooperation with private companies, combined with the vast availability of granular datasets, can inadvertently expose security agencies, personnel, and critical infrastructure to exploitation by hostile actors. The following sections outline key risk areas, highlighting how seemingly routine data acquisition practices can have profound operational consequences.

***Identification of employees in security agencies***

Even when commercially sourced data is anonymised, it can often be de-anonymised with relative ease. Commercial services exist specifically to carry out such re-identification, for instance through triangulation with other datasets. In the case of geolocation data linked to identifiers, movement patterns alone can reveal sensitive information, including a person's place of work, residence, and routine activities. A U.S. Department of Justice memorandum drew attention to the fact that journalists were able to purchase a continuous stream of 3.6 billion geolocation data points from a broker, allowing them to construct movement profiles for tens of thousands of security and military personnel, including details such as names, education, family circumstances, and hobbies.[34]

The risks arising from such exposure are multifaceted. Movement profiles can be exploited to identify physical vulnerabilities, revealing gaps in the protection of sensitive facilities that could enable espionage, sabotage, or other unauthorized access by hostile actors. Similarly, personal data derived from these profiles can be used to create compromising material for blackmail or recruitment as informants. Patterns in the data may reveal not only work-related behaviour but also private interests, health conditions, or recreational habits, providing leverage for coercion. Furthermore, foreign intelligence services could exploit linked mobile devices to deliver disinformation or malware, directly compromising the digital security of agency systems.

***Identification of vulnerabilities in critical infrastructure***

The same techniques that threaten personnel can also expose weaknesses in critical

34 U.S. Department of Justice, *Notice of Proposed Rulemaking: Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons* (2024), https://www.justice.gov/d9/2024-10/nsd_104_-_data_security_-_1124-aa01_-_notice_of_proposed_rulemaking_0.pdf. The document referred to this publication: Sebastian Meineck and Ingo Dachwitz, *Data Broker Files: How data brokers sell our location data and jeopardise national security* (2024), https://netzpolitik.org/2024/data-broker-files-how-data-brokers-sell-our-location-data-and-jeopardise-national-security/.

infrastructure. For example, an arson attack on a power cable bridge in Berlin in January 2026 caused extensive damage, revealing vulnerabilities despite routine patrols by security personnel. Commercially available data enables adversaries to identify vulnerabilities by analysing protective measures such as patrol routines, effectively undermining them.[35]

***Lack of trustworthiness of data traders***

National security risks are compounded when intelligence agencies acquire data without verifying the reliability of the broker. The opaque structures of the data market make it difficult to trace the origin or processing history of datasets, leaving agencies vulnerable to manipulation or errors. Inaccurate or tampered data can lead to flawed operational decisions and AI-driven analysis tools, potentially endangering personnel, infrastructure, or strategic planning.

***Leakage of confidential information***

Finally, the use of private providers creates additional risks for the protection of sensitive information. Storing and processing agency data on third-party systems can expose it to unauthorised access. Moreover, private actors may be able to infer the interests or focus areas of intelligence services based on analysts' usage behaviour, potentially passing this knowledge to adversaries. Even well-intentioned cooperation can therefore result in unintended exposure of classified or operationally sensitive information.

These concerns gave rise to a recent open call for evidence in the United Kingdom[36] and has led to the implementation of a "critical national security program" by the U.S. Department of Justice.[37] Furthermore, the U.S. Government Accountability Office has urged the Department of Defense to tackle these issues.[38] These are good and necessary initiatives, in our view. However, they have not sufficiently addressed the governments' own contributions to these risks when using ad-based surveillance technologies themselves.

## 2.4. Roadmap

As this chapter has shown, the acquisition and use of commercially sourced data by national security authorities have grown significantly in recent years. While the

35 Hannes Schrader, *Anschlag Auf Berliner Stromnetz: Kabelbrücke war monatelang nahezu ungeschützt zugänglich*.

36 UK Department for Science, Innovation & Technology, *Call for evidence outcome: Data brokers and national security* (4 December 2025), https://www.gov.uk/government/calls-for-evidence/data-brokers-and-national-security/data-brokers-and-national-security.

37 Similarly, pressing national security risks tied to the use of commercially sourced data by foreign adversaries have driven the U.S. Department of Justice's implementation of a new program to protect Americans' sensitive data. Available here:

38 U.S. Government Accountability Office, *DOD Needs to Address Security Risks of Publicly Accessible Information* (2025), https://www.gao.gov/assets/890/882289.pdf.

associated risks for fundamental rights and national security have been acknowledged in expert circles,[39] policy- and lawmakers seem to have eschewed genuine debates, let alone decisive regulatory measures to address and avert these risks.

How, exactly, should democratic states confront the challenges resulting from the momentous shift towards public-private coproduction of surveillance that underpins much of the modern intelligence tradecraft? To carve out possible reform options, one needs to first know a lot more about the current state of play of ADINT governance in different jurisdictions. For this purpose, we designed a questionnaire (see Chapter 3) that we then administered to intelligence oversight practitioners from eleven democracies. We did this to better understand how these key practitioners are assessing their current legal regimes and how they respond to this shift in intelligence practice. The results were quite revealing and are discussed in detail in Chapter 4. We then discuss recent changes to the legal frameworks for intelligence collection in four democracies, namely the United Kingdom, the Netherlands, the United States and Germany, and ask whether they manage to provide sufficient guidance to the services, the oversight bodies and the general public on the access and use of commercially sourced data (see Chapter 5). Based on our cartography of regulatory and oversight practice, we can describe patterns, emerging trends as well as significant divergences across jurisdictions. It allows us highlight good practice and offer policy recommendations that, we hope, might be useful for many regulators (see Chapter 6).

# 3. Research design

This chapter describes the research process that has helped us generate comparative findings on whether and how intelligence communities across several democracies are legally constrained to access and use commercially sourced data, and whether and how existing oversight and legal frameworks are equipped to address the various challenges this raises.[40]

## 3.1. Research process

Our work began with a comprehensive literature review, intended to map what is already known about intelligence communities' use of commercial sourced data, the relevant

39 Carey Shenkman et al., *Legal Loopholes and Data for Dollars. How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers* (2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf; Thorsten Wetzling and Charlotte Dietrich, *Disproportionate Use of Commercially and Publicly Available Data: Europe's next Intelligence Reform?* (2022), https://www.interface-eu.org/publications/disproportionate-use-commercially-and-publicly-available-data-europes-next-frontier.

40 We include a separate research design chapter in this report because findings on the arcane world of intelligence collection and its governance are not readily available and we wanted to be transparent on how we structured our work.

legal frameworks in place, and the state of oversight practice across democratic jurisdictions. This review drew on publicly available sources including parliamentary records, court decisions, oversight body reports, civil society publications, and academic literature.

Building on this initial review and prior research,[41] we then developed a comprehensive assessment scheme (see Section 3.3.) to better account for key dimensions, challenges and risks that lawmakers and oversight practitioners should consider when regulating, reviewing and auditing intelligence communities' access and use of commercially sourced data. The scheme helped to structure a detailed questionnaire (see Annex) that we administered to the individual representatives of intelligence oversight bodies that form part of the European Intelligence Oversight Network (EION). We also invited these practitioners to a collaborative workshop that we organised at the Council of Europe in May 2025. It brought together representative from twelve oversight bodies across European and North American democracies. Ten delegations submitted detailed written responses which we compiled and reviewed systematically ahead of the event.

The analysis of response patterns and open questions informed the agenda and discussion points for the workshop. The event was very interactive and gave us enough room to explore in further depth the responses received. Following the workshop, we produced a detailed protocol of the discussions.

Representatives of the following intelligence oversight bodies participated in the workshop:

1. Standing Intelligence Agencies Review Committee - Belgium
2. National Security and Intelligence Review Agency (NSIRA) - Canada
3. Intelligence Oversight Board (TET) - Denmark
4. Federal Commissioner of Data Protection and Freedom of Information (BfDI) - Germany
5. Independent Intelligence Oversight Council (UKRat) - Germany
6. Intelligence Ombudsperson (ZKI) - Lithuania
7. Parliament Appointed Committee for Intelligence Oversight (EOS Committee) - Norway
8. The Swedish Foreign Intelligence Inspectorate (SIUN) - Sweden
9. Independent Oversight Authority for Intelligence Activities (AB-ND) - Switzerland
10. Review Committee on the Intelligence and Security Services (CTIVD) - The Netherlands
11. Investigatory Powers Commissioner's Office (IPCO) - United Kingdom
12. Privacy and Civil Liberties Oversight Board (PCLOB) - United States of America[42]

41 Corbinian Ruckerbauer and Thorsten Wetzling, *Informationsbeschaffung mit der Kreditkarte: Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen* (2024), https://www.interface-eu.org/publications/nachrichtendienstliche-datenkaeufe

42 The participant whom we invited from PCLOB did no longer work for this institution at the time of the workshop.

In addition, we invited an academic expert and former intelligence practitioner to respond to the questionnaire and to participate in the workshop. Three individuals from the Council of Europe's Data Protection Unit joined the event as well.

## 3.2. Key terms

One of the most striking findings from the review of pertinent literature was the sheer diversity of terminology employed across different jurisdictions to describe the same or closely related phenomena. Different legal and policy frameworks refer in different ways to what is essentially a similar practice, namely the acquisition and processing by intelligence actors of personal data originating from commercial sources. We came across terms such as Advertising-based Intelligence / Advertisement intelligence (ADINT), Commercially Sourced Intelligence (CSINT), Commercially Available Information (CAI), Third Party Bulk Personal Datasets (3PD), Collateral Telemetry Data,[43] and Ad-Based Surveillance Technologies.[44] In the U.S., the concept of Ubiquitous Technical Surveillance (UTS) has also featured prominently in recent hearings and policy discussions.[45] Many civil society organisations and advocacy groups refer more plainly to data broker information.[46]

Throughout this report, we decided to use the term *commercially sourced data* to denote information that is typically collected and aggregated by data brokers as part of their involvement in the ad tech ecosystem. This includes primary or secondary information collected through real-time bidding (RTB) processes,[47] software development kits (SDKs), and telematics systems. The term is intentionally broad: it is designed to capture additional source types of data that may form part of other transactional or contractual arrangements between private sector entities (PSEs) and intelligence community actors. We find that this framing is flexible enough to encompass the range of commercial data practices relevant to the questions addressed in this report without prematurely foreclosing analysis by importing the assumptions embedded in any one jurisdiction's legal vocabulary.

43 According to the U.S. Department of Defense, this is a "a consensus term developed by the Intelligence Community to standardize reference to commercially available datasets. Such datasets could include but not be limited to advertising technologies, real-time bidding, software development kit, telematics, Internet of Things, and other related datasets under U.S. government control", U.S. Government Accountability Office, *Actions Needed to Strengthen Program Oversight and Manage Risks* (2024) https://www.gao.gov/assets/gao-24-106190.pdf

44 Wolfie Christl et al., *Uncovering Webloc: An Analysis of Penlink's Ad-based Geolocation Surveillance Tech* (9 April 2026), https://citizenlab.ca/research/analysis-of-penlinks-ad-based-geolocation-surveillance-tech/.

45 See e.g. the hearing on "Threats and Challenges Posed to Department of Defense Personnel

46 Brennan Center for Justice, *Closing the Data Broker Loophole* (2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.

47 Lena Cohen, *Online Behavioral Ads Fuel the Surveillance Industry—Here's How* (6 January 2025), https://www.eff.org/deeplinks/2025/01/online-behavioral-ads-fuel-surveillance-industry-heres-how.

## 3.3. Assessment scheme

To guide our own thinking and to help structure the ensuing comparative assessment, we developed a general analytical scheme. It emerged from an iterative process of reviewing legal frameworks and reflecting on our prior research. A recurring challenge during our work was the need to distinguish more clearly between the various stages and key moments in the relationship between intelligence community actors and private sector entities. The interactions are not uniform, since they span across different phases of the data lifecycle and their legal implications vary depending on different levels of autonomy in the data processing and the degree of their interference with fundamental rights.

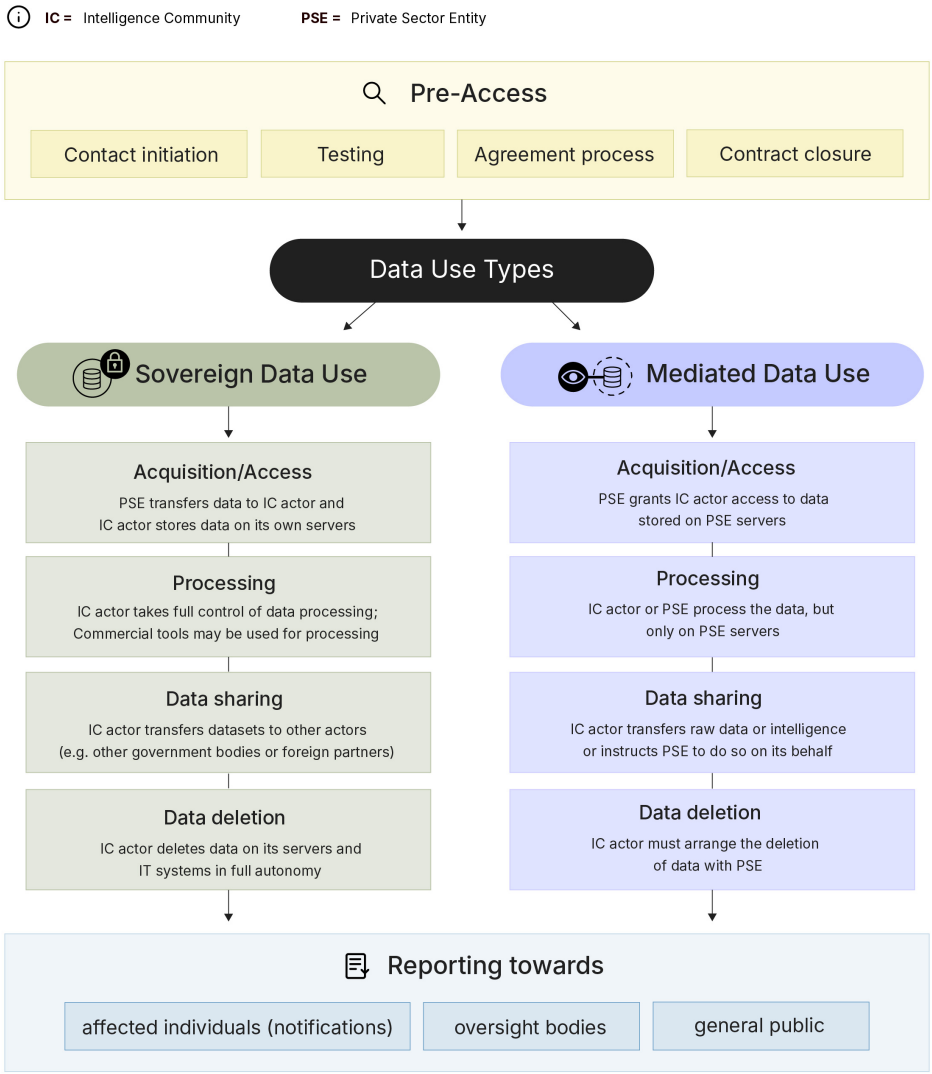
The scheme below aims to capture the various stages of this complex interaction. It includes the pre-access phase, the acquisition/access, processing, sharing, and deletion phase. The scheme allows to draw attention to nuances on how such co-operation is reflected (or not) in public and individual reporting processes. Notice that its primary focus lies on the dimensions that give rise to risks to fundamental rights. The scheme does not claim to be exhaustive. We used it as an analytical tool to help structure the discussions around a complex evolving practice and its ramifications for those designing, reviewing and implementing legal frameworks and oversight remits.

Central to the assessment scheme is a distinction between two *modi operandi* that intelligence actors typically adopt to access commercially sourced data. The first is what we refer to as *sovereign use* where an actor of the intelligence community (IC actor) acquires commercially sourced data and stores it on its own servers and IT-systems. In this mode, the security agencies have full control over the data and its subsequent processing, sharing and deletion. The private company has no further direct involvement in how the data is handled. The second mode we refer to is *mediated use*, in which the private actors grant the security agencies access to data that remains stored on the private companies own servers. In these cases, the intelligence actor interacts with the data through systems and interfaces provided by the private actor, and the degree of autonomy available to the agencies in managing the data may vary considerably. In the most extensive form of mediated use, intelligence services may simply receive finished intelligence products, derived from commercially sourced data without ever directly assessing the underlying dataset.

This distinction matters for regulation and oversight in several respects. The legal authorities required, the risks to the protection of fundamental rights and national security they entail, the oversight access available and the redress options provided differ substantially depending on the mode in which CSD are accessed by the intelligence agencies. This said, the two modes are likely to be more intertwined in practice: the same intelligence actor may operate according to a different operational mode with different

PSE entities or even for different phases of the data lifecycle. The assessment scheme takes these variations into account.

**Analysis scheme on intelligence agencies' use of commercially sourced data**




## 3.4. Description of phases

The assessment scheme structures the co-operation of private actors and security agencies into a sequence of distinct phases, each of which carries its own risks and implications for the regulator and the oversight bodies.

| Phases | Description |
|---|---|
| Pre-access | Prior to accessing data or information generated or held by private sector entities a series of preparatory interactions typically take place between intelligence services and commercial data providers. These interactions are not merely administrative: they may give rise to interferences with fundamental rights themselves and should therefore be reflected in both legal frameworks and oversight practice. Broadly speaking, the pre-access phase can encompass four different dimensions.<br>• **Contract initiation**: Initial contact between PSE and IC actor;<br>• **Testing**: IC actor receives a sample of a dataset/subscription feed and processes data to determine whether to purchase the dataset or acquire a license from PSE;<br>• **Agreement process**: IC actor is convinced of the value of the data and wants to enter a contractual relationship with PSE;<br>• **Contract closure**: IC actor and PSE become contractual partners. This forms the primary basis for the transfer of customer records, geolocation data or sensitive information about individuals in exchange for money or other things of value (such as benefits, tax advantages, and gifts). |
| Access | The access phase concerns the modalities by which IC actors obtain commercially sourced data from PSEs. For the direct (sovereign) data use, where an IC actor stores commercially sourced data on its own servers, there needs to be a prior transfer of data from a private company. Under mediated data use, the private actor grants the security agency access to data that remains stored on the security agencies own servers or third-party IT infrastructure, in return for payment or other things of value. |
| Processing | Once commercially sourced data has been acquired or accessed, it may be processed in numerous ways. This phase carries substantial risks and represents one of the most critical points at which regulation and oversight should intervene to ensure that data handling is lawful, necessary, and proportionate.<br>In the case of sovereign data use an intelligence agency takes full control of data processing once the data has been integrated into its own systems. The private company has no direct involvement in how the data is subsequently handled. It is worth noting, however, that IC actors may themselves use commercial tools and software for processing purposes. This introduces another layer of commercial dependency. In the case of mediated data use, the private company retains control over the data, and the intelligence actor interacts with privately run systems either to process the data directly or to have the data processed by the private actor on the agency's behalf. The degree to which the service provider exercises autonomous judgment in managing and processing the data may vary considerably across arrangements. In the most extensive form of mediated use, intelligence services may purchase finished intelligence products derived from commercially sourced data, without ever directly accessing or processing the underlying dataset, raising questions about accountability for the analytical judgments embedded in such products. |
| Data sharing | Once commercially sourced data has been processed and relevant intelligence extracted, intelligence agencies may determine that the resulting information needs to be shared with other government actors, foreign intelligence partner agencies, or private actors. The sharing phase raises questions about the legal basis for onward transfer, the controls applied to the information once shared, and the obligations that apply to recipient actors.<br>Under direct data use, the security agencies may transfer processed intelligence or the full dataset to other actors after completing the processing on its own IT-systems. Under mediated data use, the transaction pathways are more complex. An intelligence agency may transfer the results of data processing or finished intelligence from PSEs to a third party; alternatively, it may instruct PSEs to directly grant access to a third actor with whom the security agency wishes to share the data or intelligence. Each of these pathways involves different legal and oversight requirements and dimensions. |
| Data deletion | The deletion phase concerns the circumstances under which commercially sourced data is removed from the agencies' and private actors' systems, and the obligations, legal and practical, that govern this process.<br>Under direct data use, an intelligence actor may delete commercially sourced data from its own IT-systems and servers when it determines that the data is no longer needed or when applicable data retention requirements so require. In this mode, the intelligence actor can act unilaterally and does not need to consult the private sector entity. Under mediated data use, deletion must be coordinated with the private actor. The timely and comprehensive deletion of data depends on the scope of the access arrangement and |

| | |
|---|---|
| | the degree of control an intelligence agency retains over the dataset. This raises a significant accountability concern: where the security agency has limited control, it may be unable to guarantee that data pertaining to individuals is effectively deleted when legally required.<br>Closely related to deletion is the question of effective remedy: Where data has been unlawfully acquired or processed, or where retention has exceeded what is legally permissible, affected individuals may have a right to seek redress. The practical availability of such remedies, including the ability of oversight bodies to order or verify deletion, varies considerably across jurisdictions and is identified by the assessment scheme as a critical accountability challenge. |
| Reporting | This final phase of the assessment scheme concerns the obligations of the government agencies to report on their use of commercially sourced data and, where required, to notify affected individuals. Transparency and notification obligations serve two functions. On the one hand, they enable public accountability for the use of intrusive data practices. On the other, they create the conditions under which affected individuals can seek redress.<br>Oversight bodies play an important role in this phase, too. They may need to satisfy a legal requirement to inform the public, parliament and the government about intelligence agencies' use of commercially sourced data in their regular reports on oversight activities. In the absence of such a formal requirement, they could choose to be proactive and shed light on the agencies' acquisition and use of commercially sourced data. Chapter 5 illustrates in further detail how impactful oversight bodies can be in this context. |

The following table lists key oversight dimensions per phase. It is not meant to be mandatory.

| Phase | Oversight dimension |
|---|---|
| Pre-access | Ex-ante authorisation of data purchases |
| | Formal mandate to oversee pre-access phase |
| | Power to delay or stop the conclusion of contracts |
| | Access to executive decrees or internal administrative policies on the use of CSD |
| | Mandate to conduct investigations into internal policies and/or statutory provisions on the acquisition of CSD |
| | Public reporting on the scope of data purchases |
| | Are IC actors or governments obliged to inform oversight body about the conclusion of contract? |
| Access | Oversight of IC' access to CSD |
| | Reporting on mediated/sovereign CSD access |
| | Overview over data transferred to PSEs for processing |
| Processing | Ability to trace data minimisation efforts |
| | Knowledge of data categories present in datasets |
| | Evaluation of IC's data integrity tests |
| | Access to log recordings on the processing of CSD |

| | |
|---|---|
| | Assessment of tools used by PSE to process CSD |
| | Oversight over data sharing practices with PSEs |
| Sharing | Overview of data transfers to international partners |
| | Investigate illegal or disproportional data deletion practices |
| Deletion | Binding power to order the deletion of data |

We now turn to our empirical findings on how oversight practitioners assess the suitability of their national legal frameworks and their corresponding oversight practice for the challenge at hand.

# 4. Findings on oversight practice

## 4.1. Preface

This chapter presents and discusses information that individual intelligence oversight practitioners from ten democracies in Europe and North America gave in response to our questionnaire (see Annex).[48] It also draws on additional material obtained during the workshop where we followed up on individual responses and discussed preliminary results with the group.

The first sections focus on information received for each stage of public-private interaction on commercially sourced data as conceived in our assessment scheme (see Section 3.3.). Afterwards, the text summarises key findings and our observations on the practitioners' remarks on their national legal framework, their oversight mandate and the practice of their institutions.

We thank all workshop participants for taking the time to fill out the questionnaire and for offering their unique expertise during the workshop. Having conducted this work under the *Chatham House Rule*, the text refrains from naming individual participants or the body they represent.

48 Not every delegation or practitioner from the oversight bodies that participated in the workshop filled out the questionnaire.

## 4.2. Pre-access phase

### Our questions and their rationale

The first set of questions focused on the interaction between intelligence actors and private sector entities prior to a formal contractual relationship. We included this phase because several challenges and risks should be considered *before* a formal cooperation between an IC actor and a PSE is established on government access to commercially sourced data. For example, IC actors, and by extension oversight bodies, may only have limited access to such data prior to the actual purchase or paid subscription to a service. There is a risk, therefore, that impact assessments on privacy and other fundamental rights might either not be administered at all or only draw on partial information. Given the likely interferences with fundamental rights and the risks for national security when IC actors obtain sovereign or mediated access to such data, even at a trial stage, we probed oversight practitioners about their oversight mandate and corresponding practice:

- Does the formal mandate of the oversight body cover the pre-access phase?
- Does the national legal framework require prior authorisation for data purchases? If authorisation is required, does it involve a body independent of the executive branch?
- Do oversight bodies have comprehensive access to internal policies or executive decrees that specify how IC actors can access data held by commercial vendors?
- Do oversight bodies have access to individual contracts between IC actors and private companies? If so, can they also access draft contracts and require amendments before a contractual relationship is finalised?
- Where the oversight mandate extends to the pre-access phase, have oversight bodies conducted investigations or audits in this area? If so, are the findings included in public reports?

Regarding their national legal framework, we wanted to know:

- Does it contain provisions that prohibit, restrict, or otherwise condition IC actors' purchase of different types of data from commercial vendors?

- Are IC actors allowed to conduct business with any type of data broker, or are there restrictions concerning:
  – the provenance of the data;
  – the vendors involved;
  – the methods used to collect the data?
- Do sufficient restrictions and safeguards exist to protect sensitive information during the pre-access phase?

There are, of course, additional risks that warrant scrutiny in the pre-access phase. For example, concerns about the accuracy of commercially sourced data should be taken seriously – especially where such data is likely to be triangulated with other datasets to

which the government has lawful access, or when it is being used to train machine learning applications.

## Insights on the pre-access phase

The following sections expand on insights derived from the analysis of questionnaire responses and the workshop discussions on the pre-access phase.

**Few explicit restrictions on the purchase of CSD in national legal frameworks**

When asked whether there are any explicit prohibitions, restrictions or limitations in their country's regulatory framework regarding the types of commercially sourced data or service providers that can be used (Question 3), six country delegations indicated that this is currently not the case in their respective jurisdictions.

Some representatives mentioned that their current legal framework contains broad provisions on the use of publicly available information by IC actors and that there is much room for interpretation whether to also subsume commercially available information under these provisions. Other representatives indicated that they currently do not have sufficient guidance on the demarcation between publicly available information and commercially available information. This challenge is supported by public reporting of oversight bodies. The Canadian independent oversight body NSIRA, for instance, has warned that a requirement to ensure "that information contained in publicly available datasets does not contain information for which there is a reasonable expectation of privacy" to mitigate the privacy risks relating from commercially available information.[49]

A participant from the United States mentioned a loophole in their national legal framework that needs fixing: While the national legal framework generally prohibits companies from divulging content data without a warrant, and companies may only provide geolocation information directly to the government if the government obtains a court order,[50] there is no such restriction prohibiting companies from providing geolocation data to private companies. As a result, private companies are able to sell geolocation data to data brokers and the government, in turn, is able to buy geolocation data from data brokers.

**Mixed results regarding the question whether oversight bodies' mandate formally extends to the pre-access phase**

49 National Security and Intelligence Review Agency, *Review of Canadian Security Intelligence Service Dataset Regime* (2024), https://nsira-ossnr.gc.ca/en/reviews/find-a-review/21-15/report/.

50 18 U.S. Code §2702. See also this letter by a group of U.S. privacy and civil liberties advocates, especially on point 2: ACLU et al., *Letter to U.S. House Judiciary Committee* (10 December 2025), https://cdt.org/wp-content/uploads/2025/12/FISA-702-Reform-Priorities-Coalition-Letter-4.pdf

Asked whether their institutions are formally mandated to oversee IC activities related to the pre-access phase (Question 7), the participants gave mixed responses. Half of the answers indicated that the remit of their oversight body covers the pre-access phase while the other half stated the opposite. Interestingly, one participant cautioned that the procurement of commercially sourced data *prior* to concluding contracts is a major source of concern for them, for example, when new technologies are being tested in cooperation with PSEs.

**Seemingly robust access to relevant internal government documents and policies - with some exceptions**

When we asked delegates whether their oversight institution can access executive decrees or internal administrative policies on the use of commercially sourced data (Question 6), we learned from ten delegations that this was indeed the case for them. This is not to say, however, that such decrees and policies exist in each jurisdiction, however.

In the workshop we then asked the group whether there are documents that are important for understanding how governments access and use commercially sourced data, but that are difficult for them to access. One representative pointed out that oversight projects needed to be approved by the board of their oversight institution. If an access request does not fall within an approved project, then the process of obtaining the documents can become more difficult and time-consuming. This is noteworthy, because the very selection and adoption of some oversight projects by an oversight bodies' board might easily become politicised.

It is public knowledge that the U.S. intelligence oversight body (PCLOB) has operated since February 2025 without the necessary quorum that is legally required for approving new oversight projects. Without a quorum, the PCLOB is also unable to issue Board oversight reports, although it is able to issue staff reports. When positions remain vacant for a longer period, as is currently the case in the U.S. (and this has occurred before),[51] then this may also make it difficult for the PCLOB to make requests for information, although U.S. agencies are required to provide information sought in connection with oversight reviews that were approved when the Board had a quorum of members.

**Prior authorisation of data purchases rarely involves oversight bodies**

We also asked oversight practitioners whether specific forms of accessing commercially sourced data are subject to ex-ante authorisation in their country (Question 2). Responses indicated that in half of the countries in our sample such authorisation is required, at least for some form of CSD acquisition. This is revealing given that the countries in our

51 Silvia Lorenzo Perez, *What the PCLOB Firings Mean for the EU-US Data Privacy Framework* (2025), Center for Democracy and Technology, https://cdt.org/insights/what-the-pclob-firings-mean-for-the-eu-us-data-privacy-framework/.

sample are among those with the most extensive intelligence regulation and oversight frameworks globally. Yet, even within this group, many reported no requirement for prior authorisation for data purchases by IC actors. On closer reflection, however, we realised that our question was not precise enough. “Ex-ante authorisation”, as we formulated it in our questionnaire, can take different forms. It can be granted by a superior within the agency, a minister or a designated member of the executive branch, or an independent body. These are, of course, significant differences and those who have filled out the questionnaire might have answered the question with different entities in mind. Hence this important question needed to be posed differently: In the workshop we thus asked for a show of hands per each delegation to find out where an authorisation for CSD acquisition is required from an independent body outside of the executive branch of government. Unsurprisingly, the results were quite different then: Only two countries indicated that an independent oversight body plays a role in such prior authorisations processes.

In the workshop a representative from an oversight institution involved in such prior authorisations clarified that the government can only acquire data, including CSD, when it is covered by a class warrant that has been approved by a Judicial Commissioner.[52] If the envisaged data concerns nationals, then the government is required to seek prior authorisation from a court. The participant then pointed out that the court process is not sufficiently transparent, however. In addition, in their view IC actors, when in court, are not facing substantial hurdles to argue that they meet the required *least intrusiveness* standard.

Another oversight body representative noted that they do not have information on the processes followed between the ministries and the services when they are accessing commercially sourced data. This oversight body has mentioned that it made recommendations for undertaking risk evaluations prior to the purchase or use of new technologies. This is particularly relevant given that data protection impact assessments are not mandatory for the intelligence services in this country.

**Almost no oversight body is notified before new contracts are being concluded**

When asked whether their institution needs to be *informed* when a contract is about to be concluded (Question 8), all delegations except one answered that this was not the case. Unsurprisingly, then, we also learned that no oversight delegation in our sample needs to be *consulted* prior to the conclusion of a new contract. What is more, all oversight institutions from our sample indicated that they are not involved in decisions to renew existing contracts.

52 New Zealand's Inspector-General of Intelligence and Security recently voiced his concern regarding class warrants that "the [NZ] Service is now getting warrants for highly intrusive activities against generalised classes of people it assesses as threats. This means decisions about who, specifically, is subjected to intensive surveillance are made within the agency, not by the warrant authorities." See: Inspector-General of Intelligence and Security, *IGIS concerned at NZSIS use of class warrants* (2024), https://igis.govt.nz/publications/media-releases/announcements/igis-concerned-at-nzsis-use-of-class-warrants.

An interesting discussion arose in the workshop on the need for oversight bodies to access and review the actual contracts between the government and private companies. Some representatives initially questioned the value added of being able to access these contracts. One representative argued that this may slow down the services, others said that their body does not have sufficient resources, both staff and timewise, to look at minor contracts. They expressed the hope that potentially the availability of AI tools could change this and help the body make sense out of such contracts.

Several other oversight bodies argued, however, that such access to contracts provides very helpful information to better understand what the agencies are doing and may include important parts of a larger puzzle. Contracts provide important clues where to look for further information. When asked what other puzzle pieces need to be looked at, the participants emphasised how important it is for oversight bodies to have comprehensive access to all information of all the services. A delegate underlined how valuable it is that all major doors are open for their institution so that they can follow leads wherever they take them without the need to justify their particular interest or the relevance of the information they seek for *approved oversight projects*. This said, the person mentioned an exception to this general rule with respect to specific instances of intelligence cooperation that involve foreign partners. What surprised most participants in the workshop was that this open-door policy for the oversight body in that country also includes the private sector. More specifically, the oversight body operating under this rule can compel private sector entities to help it with investigations and audits. This is a particularly important oversight competence that other oversight body attending the workshop seemed to lack.

**No binding powers for oversight bodies to stop the conclusion of a contract**

While some country representatives indicated that they generally need to be consulted prior to any operationalisation of automated databases, which, they indicated, applied also to commercially sourced data, almost all delegations reported that they lack a binding power to delay or to stop the conclusion of a contract (Question 9). One delegate mentioned that while their institution does not possess a binding power to prevent contracts from coming into existence or to terminate them, it can review existing contracts and make recommendations for their renewal, amendment or termination. We were unable to find out whether such a recommendation was ever made in practice, however. Also, and more importantly, if such recommendations have been made, had they then been heeded by the government?

Interestingly, the discussion also revealed how participants who initially stated that their oversight body's remit covers the pre-access phase also acknowledged several times that their institutions are, in fact, often out of the loop when it comes to important practices

prior to the conclusion of contracts which can also grant government access to commercially sourced data. What is more, oversight bodies in our sample rarely have the resources to keep abreast of all relevant contracts, let alone do they have binding powers to prevent the conclusion of contracts or to insist on significant amendments to them.

**Most oversight bodies have reviewed internal policies and assessed the legality of IC actors' different access modalities concerning CSD**

Eight out of ten delegations in our sample indicated that their institution conducted investigations into internal policies and/or statutory provisions on the acquisition of commercially sourced data (Question 10). Others shared that the legal framework itself offered very little guidance for their discussions with government. Their law, one representative said, is actually not that old but already too old for this dimension to have played a role and, accordingly, it lacks guidance on CSD access by IC actors (see Chapter 5 for a review of emerging legal frameworks on this in the United Kingdom, the Netherlands, the United States and Germany). Interestingly, that person also stated that their oversight body has had frequent discussions with the government on this and have come closer to something resembling an agreement in recent months. The person also mentioned that future reviews of the national legal frameworks are pending and this aspect will play an important part.

In sum, we learned about insufficient amounts of information, resources and powers that oversight bodies report in the pre-access phase. This is a problem, we find, because it reveals significant blind spots in oversight which needs to be more comprehensive to provide democratic legitimacy to government conduct in this area. As observed by scholars Hans Born and Ian Leigh: "without access to some operational detail, an oversight body can have or give no assurance about the efficiency or the legality of the intelligence services."[53]

## 4.3. Access and data processing phase

### Our questions and their rationale

In the access phase, the acquisition of commercially sourced data creates a number of risks. Public statements from oversight bodies across different countries have sought to raise awareness on this issue. For example, it can cause difficulties for intelligence services to define the appropriate regime and applicable safeguards for the acquisition or access of data. The risk is particularly pronounced in this context, as these novel forms of

53 Hans Born and Ian Leigh, *Democratic Accountability of Intelligence Services* (2007), https://www.sipri.org/sites/default/files/YB07%20193%2005.pdf.

data access are subsumed under existing legal frameworks that often lack the granularity needed to address their complex fundamental rights implications.

This risk is further increased when technological or personnel capacities within an organisation are insufficient, or the staff is not sufficiently trained. Oversight bodies may find it more difficult to assess whether the correct legal regime was applied if they cannot verify where the acquired data came from or how it was produced. This risk is particularly high in the context of commercially sourced data because of the heterogeneity of the data sources and types potentially contained.

The risks continue in the processing phase. As a representative of the Dutch intelligence oversight body CTIVD publicly stated,[54] it is highly relevant how data is processed once it can be used by the services. Because large datasets contain major amounts of personal data of individuals that never have or will be subject to investigations of security agencies, a sufficiently clear framework for processing is crucial. Applying the right framework is equally difficult, and thus the approach of treating bulk datasets in a comparable manner, regardless of which sources they come from, is important. Where such rules are not in place, fundamental rights are put in danger.

Another concern relates to the quality of the data. If its accuracy is not verified before processing, harmful, discriminating and erroneous conclusions may be drawn from it. Furthermore, guardrails need to be in place for situations where data analysis technology allows agents to obtain sensitive information from large amounts of seemingly innocuous data, which may in essence exceed the confines of a chosen legal basis and cause grave interferences with fundamental rights that are not sufficiently justified.

A further source of concern are the risks for operational security which are particularly pronounced in instances of mediated data access, meaning when the data itself stays on the private sector entities' servers. These parties may extract relevant data and information from how the services process data (see also Chapter 5.2), thus creating a risk for operational security. An absence of applicable processes and obligations to ensure information security and separate auditing at the vendors' side of things may thus create further risk as highlighted by the U.S. oversight body PCLOB in a 2024 report.[55]

Lack of transparency and insufficient guardrails for these forms of data protection may create risks for national security as well. This also relates to the legality assessment for oversight bodies. Assessing the legality of data that is incorporated into the IC actors' systems is challenging enough, since it is very difficult to precisely analyse the nature and

54 CPDP, *Advertisement Intelligence by European Security Agencies* (2025), https://www.youtube.com/watch?v=EdTLOQGLUVI.
55 PCLOB, *Report on the National Counterterrorism Center* (2024), https://documents.pclob.gov/prod/Documents/OversightReport/4ce093a4-d28d-4996-a35b-c11d18e19018/PCLOB%20FY2024%20NCTC%20REPORT%20-%20Completed%20508%20-%20Dec%2017%202024.pdf

origin of data, and how it was processed. This gets even more challenging, however, when oversight bodies cannot access the respective systems or no sufficient logs are being kept.

In addition, it may be challenging to access the underlying source code of data analysis, making it complicated to identify discriminating patterns. These challenges are only increased when complicated self-learning algorithms are being used. Legal scholar Ashley Deeks refers to this constellation as a "double black box".[56] The double opaque nature of commercially sourced data on the one hand and the functioning of the AI-driven tools on the other creates a particularly complex situation for the rule of law. Thus, it needs a very thorough analysis of the precise use of acquired or accessed datasets. For instance, a dataset may have very different implications for fundamental rights depending on whether it is used to train a machine learning application or analysed directly.[57]

To understand how effectively national regulatory frameworks and oversight practices are currently addressing these risks, we sought to gather the answers to the following questions:

- When intelligence agencies store or access data on private company servers rather than their own systems, can the data minimisation rules that normally apply to government-held data be bypassed?
- Are there specific standardised procedures requiring agencies to minimise the data they acquire from private companies in the first place?
- Should national legal frameworks treat data that intelligence agencies use on their own systems different than data they are accessing on the systems of third parties? If so, in what ways should the rules and oversight requirements differ between these two scenarios?
- Do oversight bodies have a full picture of what data is being transferred to private companies for processing purposes and the other way around? Are the oversight bodies able to track whether data minimisation obligations are met on private systems?
- Where there is a risk that data may be manipulated, accidentally incorrect, or structurally biased, can oversight bodies assess whether agencies are taking adequate steps to verify the integrity of their data before using it? And are agencies required to re-evaluate a dataset when significant changes have been made to it, or when substantial new conclusions have been drawn from it?
- What should agencies that acquire commercially sourced data be required to put in writing, and to whom should they report on how they have processed that information? Relatedly, can the oversight bodies institution access the processing logs for commercially sourced datasets to verify compliance?

56 Ashley Deeks, *The Double Black Box: National Security, Artificial Intelligence, and the Struggle for Democratic Accountability* (2025), https://academic.oup.com/book/59551.

57 Technological Advisory Panel (TAP) of the UK's Investigatory Powers Commissioners Office (IPCO), *AI Proportionality Assessment Aid* (2025), https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/AI-Assessment-Framework.pdf.

## Insights on the access phase

This section starts with insights pertaining to the access phase followed by insights more linked to the data processing phase.[58]

**Some overseers believe that some CSD access trajectories may allow agencies to circumvent regulations**

When we asked oversight practitioners if they believed that agencies' recourse to commercially sourced data on PSE servers allows them to circumvent important rules on data minimisation (Question 12), some delegations objected to this statement or chose not to comment. Others replied that they do see a genuine risk of this being a likely trajectory in their country.

On the question whether the current legal framework in their country obliges IC actors to maintain an inventory of all databases that they use (Question 14), two delegations stated explicitly that no such obligation existed in their jurisdiction whereas six delegations confirmed this to be the case in their respective countries.

One of the participants who confirmed the existence of an obligation in their respective legal frameworks also said 'yes' to the follow-up question whether this obligation applied also to databases run on the systems or with the support of private sector entities. The person explained that lists and data mapping have to be maintained and be kept under review for retention etc this includes datasets retained and accessed.

By and large, however, we find that the situation is not sufficiently clear in most countries in our sample. Consider, for example, the Dutch Intelligence and Security Services Act 2017 (Wiv 2017). It does not contain specific provisions on private-public cooperations regarding CSD. This said, it contains a general provision[59] that could be relevant for it obliges the Dutch intelligence services to ensure that all technical, personnel and organisational measures relating to the processing of data are in accordance with the duty of care. This, however, does not amount to an explicit obligation to keep an inventory of databases, let alone for files that may be stored on PSE systems.

With regard to the United States, we can infer relevant information from the published policy framework on the U.S. intelligence agencies' use of (sensitive) commercially available information.[60] It states in the part on data management and compliance for sensitive commercially available information (II.F) that

58 We acknowledge that some themes discussed in the access phases could have been discussed just as well in the data processing phase, and vice versa.
59 Dutch Intelligence and Security Services Act 2017 (Wiv 2017), article 24. https://wetten.overheid.nl/BWBR0039896/2026-01-01.
60 ODNI, *Intelligence Community Policy Framework for Commercially Available Information* (2024), https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf.

*"IC elements shall have in place policies and procedures that require a data management plan from the point of access or collection, throughout the data lifecycle, to disposition, based on an agency's information management policies (including, for example, a Records Control Schedule and, if U.S. person information is collected and retrieved, a System of Records Notice) or applicable law."*

This requires further unpacking: When a government agency in the U.S. is obliged to maintain a System of Records Notice (SORN), as mentioned in the ODNI Framework, it must

*"publish a notice in the Federal Register that identifies the purpose for which information about an individual is collected, from whom and what type of information is collected, how the information is shared with individuals and organizations outside/external to Treasury (routine uses), and what an individual must do if they want to access and/or correct any records Treasury maintains about them."*[61]

Notice, however, that despite the ODNI framework's mention of a SORN, public records indicate that some authorities in the U.S. national security sector are exempt from SORN requirements under the Privacy Act.[62] Given the use of the works "for example" and "or applicable law", it is unclear to us if section the relevant section in the ODNI Framework amounts to an obligation to keep a fully-fledged inventory.[63]

When we asked in the workshop whether oversight body representatives would welcome a mandatory inventory of databases that extends also to databases run at PSE level, one participant cautioned that while this would certainly be helpful, one needed to ascertain first whether such an inventory is sufficiently kept up to date. If this were not the case, it might be better to get this information directly from the PSEs. In this remark, the person alluded to the power of one oversight body in our group has, namely, to compel such data directly from the PSE provided it is deemed relevant for its audits.

Asked whether their intelligence oversight institution can trace data minimisation efforts for both the intelligence services' sovereign and mediated use of commercially sourced data (Question 17), only three delegations confirmed this to be the case. A fourth delegation clarified that they can trace this for data that is stored on the service's servers.

---

61 U.S. Department of Treasury, *System of Records Notices*, https://home.treasury.gov/footer/privacy-act/system-of-records-notices-sorns

62 U.S. Department of Homeland Security, *Privacy Act of 1974: Implementation of Exemptions; System of Records; Office of Intelligence and Analysis Enterprise Records System* (30 September 2008), https://www.govinfo.gov/content/pkg/FR-2008-09-30/html/E8-22603.htm

63 According to one participant, the requirement under section II. F. of the ODNI framework applies to files run on PSE systems and servers. Another participant with in-depth knowledge on the U.S. legal framework was not aware, however, of an explicit obligation for U.S. intelligence agencies to maintain an inventory of all databases. That person also observed that the ODNI policy framework itself does not require all intelligence agencies to adopt identical procedures. It merely obliges them to adopt certain procedures and includes details on the general conditions that have to be met for these procedures.

We conclude here that it is not just a challenge for most oversight bodies but, by and large, a sheer impossibility to assess if and how data minimisation requirements that usually apply to bulk data acquisition have come to effect for commercially sourced data that is stored on private companies' systems.

As indicated, there is a considerable risk that intelligence services use commercially sourced data that are either manipulated or unintentionally incorrect or biased. In turn, this can lead to erroneous decisions. We therefore wanted to know from the oversight bodies in our group whether they can evaluate the services' efforts to test the integrity of such data (Question 19). In response to this question, six delegations confirmed that they can evaluate such efforts by intelligence agencies. One delegation clarified, however, that this kind of evaluation needed to be done manually as they cannot access the relevant systems. This seemed like a severe hindrance to such evaluation in this day and age. Two other delegations informed us that they do not possess this capacity due to a lack of technical capacities to run independent technical tests. This said, one practitioner stated that data integrity checks rank high on the wish list of this national oversight body and that they are working towards increasing the oversight bodies' capacity in this regard so that in the near future they can do this, too. Another delegation merely stated that poor data quality is not in the interest of the agencies either.

Another interesting debate ensued in the workshop on the question what intelligence actors acquiring commercially sourced data should be obliged to document in what form and to whom (Question 22). While some oversight practitioners called for information regarding the purpose of the collection as well as the mechanics of collection and subsequent data processing, others requested more specific information regarding the justifications given for the acquisition of such data following the services' evaluation of it. Practitioners also called for more statistical information on the number and type of commercially sourced data procurements by agency and more details on the safeguards applied to them.

## Insights on the data processing phase

As indicated in our analysis scheme, there are several pressing challenges that arise in the data processing phase. It is certainly not without risks to fundamental rights when agencies choose to integrate commercially sourced data into their own systems and let their analysts process the data on intelligence services' servers using tools developed and maintained by the agencies themselves. This said, there are additional risks and oversight challenges to account for when CSD data is being processed on the IC actors' behalf but on PSE servers and possibly by contractors (see the discussion in the previous chapter).

We thus wanted to know from the oversight practitioners whether their institution has a complete overview what data is transferred to PSE for data processing purposes (Question 16). Six delegations reported that they do not have such an overview of data

transfers to PSEs whereas two delegations stated that they had such an overview. This sombre self-assessment by most practitioners in our group needs to be reckoned with, we find, when thinking of reforms to boost the effectiveness of independent oversight for newer modes of intelligence activities.

Interestingly, when we asked the group whether they believe that they have a sufficiently comprehensive overview of CSD transfers to other national or international authorities (Question 28), we learned that four delegations do not claim to have such an overview. Only three delegations reported that they feel sufficiently equipped to know about such CSD transfers within different agencies of the executive branch or with foreign partner agencies. While some delegations chose not to answer these questions, there were also interesting variations in the answers given by individual oversight practitioners to both questions. One delegation, for instance, reported that it lacked such an overview regarding transfers to PSE but had such overview when it came to CSD transfers to other government agencies and foreign partners. We also want to highlight here that only two delegations from our representative sample of advanced intelligence oversight bodies from Europe and North America responded yes to both questions.

Another important indicator for oversight effectiveness lies in the ability of oversight institutions to not just have access to the IT systems and databases of the IC actor and its contract partners but to also access the log recordings when CSD has been processed. When asked about this (Question 23), nine delegations confirmed to us that they can access such log files. One delegation qualified their confirmation by saying "we do not have systems access, however, logs of the use of the data have been made available for the purpose of oversight". Only one delegation stated that they do not have direct access to such important log files per se but could request copies of such logs related to an approved oversight project.[64] (see the discussion on "approved oversight projects" in the discussion of our findings in the pre-access phase above).

Prima facie, we did not expect such solid answers from most delegations and used the workshop to probe further on this theme. For example, we wanted to know whether the practitioners can share further information with us on the tools they use to make sense of the logs to which they are privy to. One delegation acknowledged that while they have access to log files, they are not yet in the position to effectively review these files for a lack of a corresponding analysis tool. Another participant cautioned that having access to log files without having the necessary tools for their analysis is of no use to effective oversight. Luckily for them, the person underlined, their national legal framework specifically obliges the agencies to provide the tools to the oversight body so that they can review such log files.

64 See also our remarks on "approved oversight projects" in the section discussing findings from the pre-access phase above.

This said, we learned from this participant that the oversight body still encountered challenges concerning the *de facto* realisation of the *de jure* obligation. More specifically, we learned, an IC actor has provided the oversight body with a version of a tool for log file analysis that they deemed sufficient for the intended purpose. According to the oversight practitioner, however, this was not at all the case. The person attributed this discrepancy in expectations to a lack of understanding on the part of the agencies about the oversight work that is required. The person then suggested that oversight bodies should be involved at a much earlier stage when such tools are being developed. When the practitioners were asked whether they have had any experience with double logs, we heard from two delegations that there were instances where this has become necessary. The agencies, too, we were told, have seen an internal need to create such double logs and it was generally agreed that this, too, amounts to a good practice.

Finally, on the important question whether the oversight bodies have also been able to review log files for data processing that occurred by IC actors or contracted external persons on the servers and systems of PSE entities, only one participant answered. It was acknowledged that such competencies would cause a problem for the government of that country. Put simply, IC actors there prefer to be the contact point for PSE entities and would not grant oversight bodies access to log files for the processing of data on the PSE side of things.

We posed a similar question on the oversight bodies' ability to generally understand and assess data processing that might take place at the PSE-side through IC actors or through contracted partners. Does their institution encounter difficulties assessing the tools PSEs use to process commercially sourced information (Question 24)? Many have not responded to this question, but four delegations conceded that they either do encounter substantial difficulties or that they would encounter such difficulties had they tried to seek access to a PSE which, the person added, they had not yet done. In the workshop that person also shared the concern that such an attempt would likely be met with considerable pushback from the agencies. They see this as "operational territory" outside of review remit of the oversight body. The person then also called into question whether the agencies know enough about the origins of the CSD that is being processed at the PSE-side. In the discussion, another oversight practitioner from a fifth country then stated that, in theory at least, their national oversight body should enjoy similar access to PSE-side CSD processing for national security purposes. When in doubt whom to contact at the PSE side, the oversight institution from that country can simply inquire from the IC actors about their points of contacts there which, the person also mentioned, does not take up much time and has not caused problems in the past.

Another delegate acknowledged in the workshop that the national oversight body cannot go and investigate on the premises of a third party. Ultimately, the review body is still looking at the lawfulness of intelligence agency conduct. In some instances, the person observed, the intelligence oversight body can cooperate with the national institution that

is tasked with reviewing data processing at the private sector. This is because the national law empowers both institutions to coordinate and provide assistance to one another in order to deconflict where necessary. Should there be an issue of private sector data abuse that has relevance to the national security sector then this cooperation among different national oversight institution might be used to shed further light into this. There is, however, a limit to this kind of cooperation the person conceded because classified information may not be shared with the other national oversight institution. It does work better, therefore, in the reverse direction for the other oversight institution shares non-classified information with them.

A similar argument was also made by another oversight practitioner from a different jurisdiction. The person considered the national data protection office as an important and currently underused partner for intelligence accountability. The person pointed to an ongoing enquiry by the national DPO into commercial datasets which, the person hoped, would give the intelligence oversight body a more in-depth understanding on the origins of data processed by the national intelligence agencies that they have not collected through their own autonomous means.

We were also interested to learn whether the pertinent national rules oblige intelligence services to review their proportionality assessment for the use of datasets once significant changes have been made to them - or when substantial new information has been derived from it (Question 21). We received mixed responses on this question: Whereas five countries stated that there exists such an obligation in their country, four delegations reported that no such legal obligation existed in their jurisdiction. One participant stated that a legal obligation exists to consult the oversight body when changes are being made to a dataset. Another participant clarified that all datasets that are directly handled by the agencies on their premises and servers are being reviewed and if significant changes were to be made then these changes had to be detailed in an application to renew the authorisation. It was also mentioned that the absence of a legal obligation to review the proportionality assessment does not necessarily mean that the services dot not have guidelines or procedures for this in place. They may have adopted them internally.

We also looked for guidance in the U.S. ODNI Policy Framework but did not find a provision that would amount to a mandatory proportionality re-assessment once databases have been significantly amended. While the framework mentions that "IC elements shall have in place policies and procedures that require review and re-evaluation to assess whether Sensitive CAI should be retained, and if so, whether existing safeguards are adequate"[65], the precise nature and underlying requirements of such policies and procedures are not specified further. It is also noteworthy, here, that such policies and

65 See Section II. E. in ODNI, *Intelligence Community Policy Framework for Commercially Available Information*

procedures would be administered by executive agencies and not by review bodies independent of the executive branch of government. What is more, the ODNI Policy Framework is an executive policy document and not a statute passed by the U.S. Congress. Policy frameworks and executive orders, while certainly important in their own right, can be changed or revoked more easily than statutes.

## 4.4. Data sharing phase

### Our questions and their rationale

The use of commercially sourced data by intelligence services gives rise to a set of risks related to the sharing of data with other actors. Because the transfer of information oftentimes constitutes a further interference with fundamental rights, the sharing, in particular with bodies that have coercive powers, can substantially increase the intrusiveness. Oversight bodies have – if at all – also far more limited access to this data than for data that is kept internally. When data accessed on third party system is shared with or granted access to a second domestic or foreign agency, it may pass entirely outside the remit of the body originally responsible for overseeing its acquisition. Where oversight institutions lack the legal authority or practical capacity to cooperate across jurisdictional and institutional boundaries, enforcing lawful use becomes effectively impossible. The data may be re-used, re-shared, or applied to purposes far removed from those that originally justified its purchase, without any oversight body having a clear mandate to intervene. When legal frameworks do not sufficiently limit these practices, fundamental rights risk being undermined. When oversight bodies cannot comprehend let alone investigate data transfers then this, too, increases the risk that legal standards are not being adhered to.

Against this backdrop, we wanted to inquire on the following questions:

- Is there a legal framework governing how and under which conditions commercially sourced data is shared?
- Do oversight bodies have the authority and capacity to examine how commercially is transferred to other domestic or international agencies?
- Do oversight bodies have a sufficiently complete picture of where commercially sourced data goes? How might potential gaps be closed?

### Insights on the data sharing phase

In the workshop, we wanted to know from the participants if they think that the national legal framework on intelligence in their respective jurisdictions is sufficient to address these risks. One participant felt that the risks are not very high because the services tend not to share that many datasets with external partners, let alone PSE entities, for they are

too afraid that this would reveal too much about them. Four other delegations stated that, to them, the current national regime is sufficient to address the risks mentioned. Another delegation argued in a similar vein by highlighting that the existing rules are already quite rigorous in their country and that the services are constantly complaining that the current rules are already too restrictive. The person would thus not recommend to the national parliament to add specific rules on data sharing in the CSD context. Another delegation offered a different perspective. It characterised their national legal framework as insufficient in this regard for its lack of specific rules covering the various public-private interactions in the realm of commercially sourced data.

In the questionnaire we asked delegations whether the regulatory framework in their country provided specific regulations for the sharing of commercially sourced data with (a) other government agencies, (b) international partner agencies and (c) PSE actors (Question 26). Only one delegation stated in response to Question 26(a) that specific regulations existed, whereas nine delegations replied that there were no specific regulations in their respective legal framework on this aspect. One delegation offered an additional comment by stating that IC actors have to meet the requirements for data transfers, and there are specific requirements for the transfer to other government agencies, international partners or private entities. Those requirements do not distinguish between how the IC actors got the data in the first place. The regulations for the disclosure of information are based on the subject that is to be protected by the disclosure of the information, while the collection of the data underlies its own rules. So there are no specific regulations for transfer of commercially sourced data. Another delegation pointed out in the workshop that due to newly reformed regulations in their national legal framework on intelligence collection, there is now less of a need for specific provisions on the sharing of CSD with third parties. This is because the general rules on the collection and processing of bulk datasets similarly apply now in contexts that were previously, and erroneously, deemed not to be sufficiently intrusive to merit more safeguards.

Regarding the question about regulations on transfers of CSD to international partner agencies, seven delegations replied that no specific regulation existed in their national legal framework on this. One delegation stated, again, that their relevant legal framework included such provision whereas another delegation replied here that "on some occasions" this were to be the case. Finally, seven delegations replied negatively to the question whether specific rules existed in their country on the transfer of CSD from IC actors to PSE entities. Two delegations stated that such regulations existed and one of them pointed to a specific article in the national legal framework that heavily restricts the sharing of information. In the words of this participant, "PSE entities cannot receive such information from the agencies."

Turning away from the legal framework and considering the oversight dimension, we know that most oversight activities tend to be far easier to justify and explain vis-à-vis the

government and the IC actors when they are part of the formal legal mandate of an oversight body. We therefore wanted to know from the oversight bodies represented in our group whether their official remit covers inspections and audits on the IC actors' sharing of CSD with partner institutions within government and with foreign partners (Question 27). Interestingly, seven delegations confirmed this to be the case. Only one delegation specifically stated that this is not part of the formal oversight remit, whereas some did not respond to this question. Another delegation specified that the current national legal framework does not contain provisions that specifically address CSD and public-private cooperation on this. However, general powers of the national IC to process bulk data are applicable and subject to several legal requirements, including requirements on (external) data sharing. Another participant cautioned that while data sharing with foreign intelligence services is part of their remit, this does not extend beyond the national borders, i.e. it excludes the verification of subsequent data use by the foreign intelligence service.

Despite the fact that most oversight bodies confirmed that inspections and audits on the IC actors sharing of CSD with other agencies and foreign partners are part of their formal remit, no oversight body reported to us that they had done such an inspection or audit specifically on this subject. Five delegations indicated that they had not done so whereas two delegations did not respond to the question. Two delegations specified that they had performed such audits and inspections on data sharing in other contexts of IC actors' activities. One participant cautioned that CSD is not a legally defined term in their country but referred to a recent public report of their institution that used a broader definition for automated OSINT. Given this sombre observation and the fact that some oversight bodies consider this aspect to be part of their formal mandate, as well as the recent reporting of a first documented instance of an EU country purchasing a commercial tool (Webloc) that reviews CSD,[66] we strongly encourage oversight bodies to invest more time and resources in audits and inspections on this topic.

## 4.5. Data deletion phase

### Our questions and their rationale

When data is stored on a third-party server, the intelligence services need to rely on that entity to delete data when this is legally required or when the intelligence services see a need for this. For both the services and the oversight bodies it may be complicated to verify that all copies, backups or residual data has been fully and permanently deleted.

66 Szabolcs Panyi, *Orbán's Spying Kit Revealed: Israeli Surveillance Tool Combined with Hungarian Technology* (2026), https://vsquare.org/orban-spying-toolkit-cobwebs-webloc-hungary-spyware-citizen-lab/.

Data deletion poses a fundamental challenge within the services' systems, but it becomes even more daunting in instances where the services' access to commercially sourced data is mediated. If the framework regarding the necessary deletion processes and potential record-keeping guidelines fail to address these challenge, serious risks for fundamental rights can arise from this. Sensitive data that should no longer be accessible may still be used with potentially negative consequences for numerous individuals affected.

To evaluate to what extent regulatory frameworks address this challenge and whether oversight bodies are capable to ensure legality in this phase, we asked the following questions:

- Do regulatory frameworks provide specific rules on deletion notices and recordkeeping?
- Do these rules apply as well when the data is held on third-party servers?
- Do oversight bodies have the power to investigate suspected breaches of these rules, and to formally order the deletion of data that should no longer be held, including when data is held by private companies?

## Insights on the data deletion phase

Interestingly, all but one practitioner responded that their national legal framework knows no specific record-keeping provisions regarding the deletion of commercially sourced data (Question 31). The person specified that deletions have to fulfil a statutory purpose and need to satisfy the necessary and proportionate criteria, too. When hearing about this again in the workshop, one delegate corrected the questionnaire answer by saying that record-keeping obligations are, in fact, mentioned in the national framework but they are not mandatory. Another delegate acknowledged in the workshop that such obligations would add value in the "mediated data use" scenario: Consistent policies and notices would be helpful, the person explained, in situations where the PSE is required to delete data so that the PSE can notify agency users of the deletion. In turn, this would enable the agencies to implement their own policies regarding data deletion.

Interestingly, one delegate cautioned that record-keeping can also mean that some part of the data will be kept alive. This is something that regulators and overseers should bear in mind.

With regard to oversight powers and practice, we asked the delegates whether their institution could initiate an investigation if it became aware of an illegal or disproportionate data deletion practice involving CSD (Question 33). All delegations without exception confirmed to us that their institution can do so. Yet, only two delegations replied positively to our follow-up question whether their institution had a binding power to order the deletion of commercially sourced datasets (Question 34). One delegation further specified that while it possessed a binding power to order the deletion of bulk datasets, the national framework does not specifically include the term CSD or

commercial data nor does it include provisions that apply specifically to PSEs. However, following recent reforms, the delegation explained, such powers now apply to all bulk datasets, including those obtained through powers which under the old law were deemed not to be very intrusive. Due to these changes, the delegation mentioned, there is less of a regulatory need to specifically adopt provisions regulating the deletion of bulk commercially sourced data.

Another delegation stated in response to this question that they can address a recommendation to delete a dataset to the head of the Department of Defence. If that person does not wish to implement the recommendation, he or she must then seek the approval of the entire government. This, we were also told, has not yet occurred.

In response to our follow-up question in the workshop whether that particular oversight body had ever made a recommendation to delete a CSD dataset, we learned that this was not the case. We were then also informed that this would then also pose an additional challenge to prove that such a deletion had actually taken place. Another delegate mentioned with regard to the deletion challenge that their institution is "still largely in the woods on backup technology and technologies that are resilient to deletion, so we have to find a technical solution to that first".

## 4.6. Reporting

### Our questions and their rationale

As described above, oversight bodies struggle to assess the legality of intelligence services' conduct in this space. Another problem they face in the context of commercially sourced data is that trade secrets may hinder them in accessing all relevant information and in particular to publicly report on relevant matters. In some cases it is not the trade secret, however, that seems to hinder oversight bodies in reporting publicly about their findings. Rather, it can also be that access and use of commercially sourced data as such is treated as a secret method of intelligence conduct. In both cases the lacking possibility to report publicly on this type of data access hampers public trust in the independence and effectiveness of intelligence oversight.

To better understand where national frameworks stand in the context of this challenge, we asked delegations whether they are able to report on intelligence service’s use of commercially sourced data and whether and how they have actually done so.

### Insights on this stage: Only limited reporting on the scope of data purchases

The majority of participants indicated that their oversight institution cannot publicly

report on the scope of data purchases by their national IC (Question 36). This, we were told, is mostly due to secrecy requirements. A U.S. participant explained that that if oversight bodies want to include any classified information in their reports, they must first seek public interest declassification of the information by the government. Another practitioner clarified that while the national oversight institution cannot inform the public about classified material, it goes at great length to depict such matters in its annual report. It aims to do so in a way that does not constitute a breach against the secrecy requirements but still allows the public to learn about the basic contents of the oversight institution's work. The final wording of the annual report is shared with the government ahead of publication just to be sure. Other oversight bodies have indicated that they can report publicly on this and referred to their reports.[67]

The Dutch oversight body CTIVD has made a very detailed public-facing effort when it published a report that drew attention to IC actors' access to both publicly and commercially available data. This said, the UK oversight body has also included a segment on CSD in its recent public reporting, where it acknowledged: “Part 7B applications may need to accommodate a great deal of uncertainty as to the nature and extent of the datasets that are being accessed. As, by definition, UKIC does not hold the data, it is often limited as to its knowledge of the data held by a third party. The regime also poses an inherent difficulty when it comes to being able to audit access. In many cases this might be technically impossible or highly undesirable for operational security reasons (as acknowledged at paragraphs 5.6-5.9 of the draft Code of Practice) and UKIC understandably would not wish to leave a trail of their subjects of interest. Given the requirement for a Part 7B warrant will not be commenced until April 2025, we will report on this again in our next Annual Report”[68]

Furthermore, the Norwegian oversight body has made its dissent public concerning the question whether purchases of metadata could be subsumed under the existing regulations for publicly available information.[69]

With the event of the first documented European purchase and use of advertisement-based surveillance technology in Hungary in April 2026,[70] it is hoped that oversight bodies will draw further attention to this important topic in their next reports.

67 In the U.S., PCLOB concluded its long-term investigation that started in 2020 on the FBI’s use of OSINT and commercially available data with a staff report that was published in 2025.

68 IPCO, *Annual Report of the Investigatory Powers Commissioner 2024* (2025), https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2024.pdf, p.18.

69 OA-IA, *2024 Annual Report of the Independent Oversight Authority for Intelligence Activities* (2025), https://2024.ab-nd-taetigkeitsbericht.ch/en/, pp. 14-15.

70 Szabolcs Panyi, *Orbán’s Spying Kit Revealed: Israeli Surveillance Tool Combined with Hungarian Technology* (2026), https://vsquare.org/orban-spying-toolkit-cobwebs-webloc-hungary-spyware-citizen-lab/.

## 4.7. Synopsis

Despite its increased significance, the multi-facetted forms of cooperation between intelligence agencies and private sector entities on the use of commercially sourced data remains very opaque. We designed a questionnaire and a collaborative workshop with oversight practitioners to get a better comparative understanding about the existence of legal and procedural safeguards across different jurisdictions for different access and -use modalities at different stages of the commercially sourced data lifecycle.

The following section presents key takeaways from the previous discussion. They should give policy- and lawmakers reason to advance genuine reforms to better govern IC actors' access and use of commercially sourced data.

### Caveat

The findings presented in this chapter draw on answers that individual intelligence oversight practitioners from eleven democracies in Europe and North America have given in response to our questionnaire (see Annex) as well as their responses to follow-up questions posed during the in-person workshop. We cannot infer a formal position of a national intelligence oversight body on a given theme or question solely from the responses that individual oversight practitioners provided. Having said this, the individuals who filled out the questionnaire and participated in our workshop hold unique and long-term experience in this field. This does give gravity to their responses.

We anonymised the participants' individual contributions due to the application of the Chatham House Rule.

**Uplifting results**

- Most delegations informed us that their oversight institution can access executive decrees or internal administrative policies on the use of CSD and/or data purchasing from PSEs.
- Eight delegations reported that their institutions conducted investigations into internal policies and/or statutory provisions on the acquisition of CSD.
- All but one delegation reported that their oversight body has either immediate access to IC actors' log recordings on the processing of CSD or has received such access upon request for the purpose of oversight.
- Most delegations indicated that the formal remit of their oversight institution covers inspections and audits into the sharing of CSD with partner institutions within government and with foreign partners.
- All delegations reported that their oversight body can initiate investigations if it learns about illegal or disproportionate CSD deletion practices.

- Only two delegations reported that their oversight body cannot evaluate the IC's effort to test the integrity of CSD.

**Sombre findings**

- Half of the delegations reported that their oversight bodies' remit does not cover the procurement phase. In essence, their institutions cannot review, let alone require changes or prevent the signing of government contracts with private sector entities.
- Only two delegations reported that their oversight body plays a role in prior authorisations of government decisions to acquire CSD.
- All delegations except one told us that their oversight body is not informed when new contracts are concluded with PSEs on CSD.
- No delegation stated that their oversight institution possesses a binding power to delay or stop the conclusion of such a contract with PSEs.
- Most oversight practitioners told us that their institution cannot report publicly on the scope of the intelligence communities' access to CSD.
- Three delegations stated that their oversight body has encountered severe difficulties when assessing the tools PSEs use to process CSD. Another seasoned oversight practitioner stated that they would expect such difficulties had the oversight body tried to do so, which, the person acknowledged, it had not yet done.
- Six delegations reported that their oversight body lacks a comprehensive overview of data transfers from IC actors to PSEs for data processing purposes.
- Four delegations reported that their oversight body also lacks such an overview with regard to transfers involving CSD to international partner agencies.
- Only three delegations from our sample of rather advanced intelligence oversight bodies from Europe and North America responded that they have both a sufficient overview of such data transfers to PSE entities and to international partners.
- Even though most delegations stated that inspections and audits on the IC actors sharing of CSD with other agencies and foreign partners are part of their oversight bodies' formal remit, no delegation reported that their institution had done an inspection or audit specifically on this subject.

For further illustration, the table below depicts how the majority of representatives of intelligence oversight bodies in our simple have reported on their institutions' involvement across key governance of intelligence agencies' access and use of commercially sourced data.

**Findings on oversight engagement per phase**

Mostly absent — Mixed results — Mostly present

| Phase | Oversight dimension | Findings |
|---|---|---|
| Pre-access | Ex-ante authorisation of data purchases | ✗ |
| | Formal mandate to oversee pre-access phase | — |
| | Power to delay or stop the conclusion of contracts | ✗ |
| | Access to executive decrees or internal administrative policies on the use of CSD | ✗ |
| | Mandate to review policies and bylaws on CSD acquisition | ✓ |
| | Public reporting on the scope of data purchases | ✗ |
| | IC or government obliged to inform oversight body about contract conclusion | ✗ |
| Access | Oversight of IC access to data | n/a |
| | Reporting of mediated/sovereign access | n/a |
| | Prevent the circumenvention of rules on access to personal data | — |
| Processing | Overview over data transferred to PSEs for processing | ✗ |
| | Ability to trace data minimization efforts | n/a |
| | Knowledge of data categories present in datasets | n/a |
| | Evaluation of IC's data integrity tests | ✓ |
| | Access to log recordings on the processing of CSD | ✓ |
| | Assessment of tools used by PSE to process CSD | ✗ |
| Sharing | Oversight over data sharing practices and partners | — |
| | Overview of data transfers to international partners | — |
| Deletion | Investigate illegal or disproportional data deletion practices | ✓ |
| | Binding power to order the deletion of data | n/a |

Sovereign Data Use — Mediated Data Use

## 4.8. No need to adjust current legal frameworks?

Beyond the more pointed questions regarding different legal and procedural safeguards at different stages in the CSD lifecycle, we also posed general questions to the participants regarding their preferred design and scope of legal provisions to govern future use of CSD by their national IC. This section briefly discusses insights drawn from practitioner responses to these more general questions. It is instructive, we believe, to juxtapose the different views on the general suitability of current national frameworks with the more granular insights on the existence of legal and procedural safeguards for different stages of CSD-access and use (see Sections 4.2 and 4.3).

## Various views on different regulation challenges

The questionnaire and the corresponding workshop allowed us to tap into different angles that need to be considered when thinking of improving the current state of play regarding regulation and oversight on IC actors' use of CSD. There are questions about the right degree of granularity that lawmakers should aspire to meet when crafting individual provisions to govern the future recourse of IC actors to CSD. Should they aspire for density and comprehensiveness or flexibility with a view to the end users of such legal provisions? A key question related to this was whether it is useful for legal frameworks to distinguish clearly between what we called sovereign and mediated access and use of CSD for national security purposes (see the assessment scheme introduced in Chapter 3.3).

Another question is whether ADINT practices and the ensuing risks to fundamental rights and national security are so substantial that provisions governing IC actors' activities and corresponding oversight and accountability mechanisms ought to be placed on a statutory footing adopted by parliament rather than in government policy frameworks or executive orders. Finally, at least for the European participants in the workshop, the question arose whether the EU's General Data Protection Regulation (GDPR) is a sufficient legal instrument to prevent problematic CSD to enter the data market in the first place.

## Oversight practitioners disagree on the question whether separate legal provisions for sovereign and mediated access to CSD are needed

Asked whether there should be different regulations and oversight requirements in the national legal frameworks for "sovereign data acquisition" and "mediated data access" (Question 13), we received a mixed bag of responses. The majority of delegations responding to the questions told us that they do not think that there should be separate legal regimes for this. By contrast, two practitioners expressed their support for the creation of two separate legal regimes. A third delegation indicated that it would be sufficient to add new legal provisions to the existing legal framework.

We discussed this further in the workshop and heard additional arguments in favour of each position. We learned, for example, that in the mediated access modality where CSD is stored on PSE servers there is a lower risk that IC actors will cause a data breach or engage in improper secondary use of such data. However, a person also cautioned: IC actors are also less in control of the data and their ability to ensure data minimisation obligations are being adhered to (e.g. through masking the identities of individuals) is also much more limited. Future lawmakers, the person insisted, need to ensure that IC actors do not simply avoid the rules that otherwise apply to government actors by availing

themselves of the mediated data access route. Hence, legal provisions are indeed needed, the person underlined, to make sure that key safeguards are being applied and that data access remains restricted and documented, for example.

Another oversight practitioner agreed to this and stated that due to the current risk of data minimisation circumvention, different requirements should apply for mediated data access compared to sovereign CSD acquisitions. Another participant simply stated that the national parliament should make it clear in the national legal framework for intelligence itself which kind of CSD and which kinds of contracts and non-compulsory relationships between IC actors and PSE should be allowed. This person also added that, at present, the members of the oversight body are under the impression that at least the parliament does not have enough knowledge of the details and the risks concerning this topic.

Apart from the question whether separate legal regimes should be adopted to regulate the different CSD access and use modalities for national security purposes, we also inquired about the degree of granularity and flexibility that amended legal frameworks should provide for the different stakeholders in the governance of ADINT. We had an interactive discussion in the workshop on this question and one participant mentioned that all the necessary elements of foreseeability and proportionality should be addressed. The provisions should contain clear definitions and oblige IC actors to define queries, subject them to logging and they should also obliged to appoint designated and trained employees to work with CSD. Legislation has limits if it becomes too prescriptive and IC actors will find the path of least resistance. Thus, the person concluded, in a multi-conditional and multi-player environment such as modern ADINT practice, you might get a compliance result quite different to what the oversight body had in mind.

Another practitioner from a different country agreed and deplored that there currently is no specific national legislation for IC actors' access and use of CSD. The person cautioned, however that the legal framework should be a more general one without too much specification. This is because the oversight body in question oversees a variety of different agencies which are subject to numerous different laws that were adopted at different points in time. To align them all under too granular provisions for rule-based conduct would be extremely difficult, the person cautioned.

There is, however, a clear need for the establishment of minimal standards, the person stated, whereby the IC as such would also make sure that it did not vary too much in terms of its acquisition and handling of CSD. What is more, it should also ensure that individual IC actors do not conclude vastly different contracts with similar PSEs for comparable services. Another delegation deplored that in their respective jurisdiction there is currently no legal provision that offers guidance to the IC actors under which circumstances they can acquire CSD in the first place.

Moreover, an additional important aspect was mentioned by another practitioner who cautioned that intelligence agencies often complain that too rigid legal provisions will be counter-productive from a national security perspective. If their adversaries can have rather unhindered access to CSD, the national task should be to find a legal way for them to get access to this data, too. Hence, agencies will certainly fight back on a too prescriptive law. Having no law in place and resting the governance merely on executive orders and policy frameworks, the person acknowledged, is becoming even less advisable in situations where the executive branch of government is frequently changing its strategic objectives. A U.S. practitioner argued in a similar vein and explained that to ensure jurisdiction for the national courts to provide judicial oversight, there needs to be legislation. U.S. courts do not have jurisdiction to enforce executive orders. In addition, while executive decrees or orders are binding when they are in effect, these are a lot easier to change than statutes. Hence the need for a proper statutory footing and codification.

The discussion also focused on the usefulness of existing supranational data privacy regulations such as the European Union General Data Protection Regulation (GDPR). Some practitioners saw value in the GDPR for the challenge at hand, despite its broad national security exemption. GDPR could become part of the solution for the better governance of mediated CSD access, one participant stated, should PSEs fall under its regime for data processors. If this were to be the case than intelligence agencies simply needed to make sure that there is no difference between the requirements of the intelligence community and PSEs when it comes to data handling. The problem, however, comes when the data processor category in the GDPR cannot be applied to PSEs such as data brokers. Then PSEs could not be held to the more stringent responsibilities under the GDPR. Based on the persons' deliberations with legal experts and colleagues, there is, unfortunately, a probability that the GDPR has a loophole in this regard. Hence, to date, there is a clearer legal path to sketch when the intelligence agency integrates the data into their system. Yet when an intelligence agency does not, in the strict sense, obtain access to the data but has PSE actors acquire CSD on their behalf from actors who may not even fall under the GDPR data processor category, then it is much harder to enforce more stringent restrictions.

Another participant mentioned in response to this that their national parliament has adopted a special legal regime specifically applicable for intelligence services when integrating GDPR in national law. It has incorporated the principles of the GDPR but gives agencies more leeway when it comes to the storage of sensitive data, for example. Yet, they still must adhere to general data minimisation standards expressed in the GDPR, for example.

Naturally, the discussions on the right kind of ingredients and granularity of national legal frameworks go beyond the results of our findings from the questionnaire that we administered to the practitioners of intelligence oversight. The next chapter, therefore, looks more closely at emerging legal frameworks in four democracies.

# 5. Different approaches to regulation

Where do different democracies currently stand when it comes to the regulation of their intelligence services' acquisition, access and use of commercially sourced data Have national parliaments already amended intelligence laws to fully reflect the paradigm shift in modern intelligence practice and the need for regulation and control

This chapter answers this question, at least in part, with the help of a comparative overview of how the etherlands, the United ingdom, the United tates and ermany sought to meet the regulatory challenge. ur discussions with oversight practitioners have influenced our case selection. We knew that some countries, such as the United ingdom, have recently amended their national intelligence legislation while others, such as the United tates, adopted new policy frameworks. takeholders in the etherlands have been very explicit in their criticism of the existing legal framework and the need for regulatory adjustments. ermany, by contrast, seemed like a good country to include into this sample because it has not, at least to our knowledge, been at the forefront of legislative reforms or oversight practice when it comes to the intelligence agencies' acquisition, access and use of commercially sourced data.

ther jurisdictions face similar challenges, too. More case studies are thus in order, but our resources did not allow for this. We encourage readers to alert us to interesting developments in their jurisdictions. Time and resources provided, we plan to create an online repository where further information will be listed. This said, the four different national cases presented in this chapter capture a broad range of different reform trajectories.

efore we begin, we need to recall that national security remains one of the least harmonised policy areas. Few national responses to legal and administrative challenges are readily transferable to other jurisdictions. till, certain national approaches discussed below may serve as a valuable source of inspiration in other jurisdictions, too. We encourage legislators to join the common quest for a more rights-based governance of a field that is woefully under the radar of most parliaments in urope to date.

## 5.1. The Netherlands

The etherlands, and in particular its independent oversight body for intelligence services, CTIVD, has been a pioneer in addressing the challenges of commercially sourced data in public. With the help of its public reports, CTIVD contributed to the dynamic evolution of intelligence legislation on the collection and processing of bulk

datasets in recent years.[71] As in other European countries, Dutch intelligence legislation is currently under review, and the forthcoming reform is likely to reform not just the legislative framework for intelligence collection but also the design of the oversight architecture.

For example, the new Dutch government announced in its coalition agreement that it seeks to merge the two oversight bodies TIB (currently performing ex ante oversight) and CTIVD (currently performing ex nunc and ex post oversight), with yet uncertain consequences for the pursuit of current and future oversight mandates and powers.[72] The government has further announced plans to substantially strengthen the two Dutch intelligence services, the military intelligence service (*Militaire Inlichtingen- en Veiligheidsdienst*; hereafter MIVD) and the civilian intelligence agency (*Algemene Inlichtingen- en Veiligheidsdienst*; hereafter AIVD), by enhancing their technological capabilities and improving cyber threat detection through greater integration of data from public and private organisations. It appears likely that some of the private-public cooperation regarding commercially sourced data discussed in this report will form part of such efforts.

## The Wiv 2017

When originally enacted, the Dutch Intelligence and Security Services Act 2017 (Wiv 2017) introduced a tiered legislative framework for acquiring data. The presumed sensitivity of the data, and accordingly, the safeguards applied, depended on the method of collection. In this structure, a distinction was drawn between general powers and special powers, the latter being regarded as involving a more serious interference with fundamental rights. Within the scope of this report, data acquisition from commercial sources may arise under four distinct powers: collection of data from publicly accessible information sources (Art. 25), the systematic collection of data from publicly accessible information sources (Art. 38), the informant-power (Art. 39) and the agent-power (Art. 41).

**General vs. Special Powers in the Wiv 2017**

71 CTIVD, *Toezichtsrapport Nr 79 over de Inzet van Virtuele Agenten door de AIVD en de MIVD* (2024), https://www.ctivd.nl/documenten/2024/09/09/index; CTIVD, *Review Report no 74: Automated OSINT: tools and sources for open source investigation* (2021), https://english.ctivd.nl/documents/2022/09/19/index.

72 D66, VVD, and CDA, *2026-2030 Coalition Agreement: Let's Get to Work. Building a Better Netherlands* (2026), https://www.government.nl/documents/publications/2026/02/23/2026-2030-coalition-agreement-lets-get-to-work---building-a-better-netherlands.

| | General Powers | | | Special Powers |
|---|---|---|---|---|
| Data collection method | Non-systematic collection from publicly accessible sources | Systematic collection from publicly accessible sources | Informants | Agents |
| Legal basis | Article 25 Wiv 2017 | Article 38 Wiv 2017 | Article 39 Wiv 2017 | Article 41 Wiv 2017 |
| Description of method | Collection of publicly available personal data with or without a technical tool. | Systematic collection of data on individuals from publicly accessible sources, including through automated tools, e.g. web scraping, API use | Asking an informant to share information. The informant cooperates on a voluntary basis, applying pressure is not allowed. | Agent cooperates on a voluntary basis, applying pressure is not allowed; following an application for the deployment of agent power, the agent acts upon specific instructions of the Intelligence service to gather specific information. |
| Delineation criteria from other data collection methods | Publicly accessible data | Publicly accessible data + likely to generate comprehensive overview of particular element of an individual's private life | Data collected from persons not directed or instructed by intelligence service | Agents are natural persons under the responsibility and instruction of the intelligence service; includes intelligence service instructing non-employees |
| Authorisation process | – | Minister or head of a service on their behalf. The head of the intelligence service may designate subordinate official– copy is to be sent to the responsible minister | Legal basis does not require prior authorisation; internal policies require head of intelligence service or minister approval for special categories[73] | Ministerial approval or approval by head of a service on their behalf. The head of the intelligence service may designate a subordinate official; a copy is to be sent to the responsible minister |
| Involvement of independent oversight body in authorisation | - | - | - | - |
| Additional safeguards | - | - | Use of informants needs to meet the tests of necessity, proportionality and subsidiarity | Preparation of acquisition memorandum testing necessity, proportionality and subsidiarity prior to agent commissioning, deletion requirements for protected data |

## Loopholes and shortcomings of the Wiv

In a report on the use of automated OSINT tools published in 2022, CTIVD made it clear that the existing provisions of the Wiv 2017 were not adequate to cover the serious interferences with fundamental rights arising from the intelligence services' activities in this field. According to the oversight body, automated OSINT tools were, at the time, capable of enabling searchable access to "hundreds of sources of various origins, including location data or data from leaked data sets".[74] Against this background, CTIVD recommended the establishment of "a more foreseeable legal basis with sufficient safeguards governing the use of automated OSINT for both the tools themselves and the sources that can be accessed using these tools".[75]

Another significant problem, according to CTIVD, was that the Wiv 2017 did not provide specific rules governing the further processing of bulk datasets. CTIVD publicly criticised this absence of safeguards, arguing that bulk datasets generally contain sensitive data relating to a large number of individuals who have never been, and never will be, under investigation by the relevant security agencies. The oversight body further observed that the sensitivity of a bulk dataset does not depend on the way it was obtained or accessed, but rather on the nature of the data it contains. It argued that the applying general data processing rules were too broad and did not sufficiently address the substantial interference with fundamental rights that the processing of such bulk might entail.

What these different access-scenarios also have in common is, that no independent ex-ante oversight is needed. Different to other special powers (such as bulk interception of telecommunication or hacking) that interfere severely with fundamental rights, not even the agent scheme requires the authorisation of the independent TIB.

## 'Bulk is bulk' and remaining challenges

In response to the criticism on the lack of safeguards for the processing of bulk datasets, the competent ministers in the Netherlands announced their intention to introduce a more coherent framework in the revised intelligence legislation. It is currently under review and a first draft of the legislation is expected to be presented to the parliament in 2026.[76]

---

73 Dutch Government, *Regels met betrekking tot de inlichtingen - en veiligheidsdiensten alsmede wijziging van enkele wetten* (2018), https://zoek.officielebekendmakingen.nl/kst-34588-79.html.

74 CTIVD, *Review Report no 74: Automated OSINT: tools and sources for open source investigation* (2021), https://english.ctivd.nl/documents/2022/09/19/index.

75 CTIVD, *Review Report no 74: Automated OSINT: tools and sources for open source investigation* (2021), https://english.ctivd.nl/documents/2022/09/19/index.

76 Dutch Government, *Regels met betrekking tot de inlichtingen - en veiligheidsdiensten alsmede wijziging van enkele wetten.*

As a provisional measure, the government established a Temporary Regulation (Tijdelijke Regeling) in 2020, providing additional safeguards in this regard. A guiding principle applied by the oversight body is "*bulk is bulk*", meaning that robust safeguards must apply to all bulk datasets, regardless of the manner in which they were obtained.[77]

That said, different bulk datasets may be treated differently, depending on the sensitivity assessment on which rules apply. Under the Temporary Regulation, every dataset classified as bulk must be assessed and assigned to an access regime. This applies equally to datasets collected via methods previously considered to be non-sensitive. The assessment is based on a catalogue that evaluates the extent to which the bulk dataset reveals aspects of an individual's private life, and the extent to which it is publicly accessible. The explanatory notes to the regulation identify four categories of data whose presence can elevate the overall sensitivity of a dataset:

- data that can be traced back to an individual such as names, IP-addresses or other identifying data
- location data
- data that can be used to establish connections between different individuals (such as communication meta data)
- data that reveals aspects of an individual's private life or preferences.[78]

The sensitivity assessment determines the specific rules governing the processing of the datasets and needs to be confirmed by the Minister of Defence (for MIVD) or Home Affairs (for AIVD). The CTIVD must be notified every time the minister has decided upon an access regime, i.e. whether it falls under:

- the standard access regime (Art. 5 Temporary Regulation),
- the limited access regime (Art. 6 Temporary Regulation) or
- strictly limited access regime (Art. 7 Temporary Regulation).

Depending on the precise regime, different sets of safeguards apply as shown in the table below.

| Access regime | Data processing by | Procedure for obtaining processing permission | Validity of processing permission | Review interval for mandatory deletion assessment |
|---|---|---|---|---|
| Standard access regime (Art. 5) | Analysts/ officials within the service with task-related need | No special permission required beyond necessity for task | No fixed time limit (task-based) | 36 months |

77 CPDP, *Advertisement Intelligence by European Security Agencies*, https://www.youtube.com/watch?v=EdTLOQGLUVI

78 Dutch Government, *Regeling van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie* (2020), https://zoek.officielebekendmakingen.nl/stcrt-2020-56482.html.

| | | | | |
|---|---|---|---|---|
| Limited access regime (Art. 6) | Designated specialists for bulk data analysis AND Investigatory teams following approval | Written request ought to be submitted to the head of the intelligence service; needs to provide reasons for its justification; final decision based on advice from the Legal Affairs Department | 12 months | 24 months |
| Strictly limited access regime (Art. 7) | Designated specialists for bulk data analysis AND Investigatory teams following approval | Same procedure as in limited access regime + mandatory link to a specific investigation established by the head accessing data (based on specific query characteristics) | 12 months | 12 months |

Following CTIVD's initiative and its public statements, the government filled an important gap on a framework for the processing of bulk data. While the content of data played a role in defining the precise safeguards that were to apply in the traditional legal design as well, it nevertheless played a much smaller role then. Introducing this mandatory assessment for every type of bulk data is a significant step towards a more coherent regulatory framework, closing important loopholes.

What is more, in anticipation of the revised intelligence legislation, a new temporary act entered into force on July 1, 2024.[79] This new legal regime covers various topics, including new provisions for retaining bulk data sets collected through special powers.[80] A member of CTIVD described a range of notable changes that the temporary act brought about in a public event in May 2025:

*"Based upon that law, bulk datasets obtained through special powers must still be destroyed after 18 months. However, what is new is that the services may, by way of exception, request permission from the minister to retain a bulk dataset for an additional 12 months if there is an urgent need to do so for national security purposes. To get a permission, the services must demonstrate that such a retention is necessary and proportionate and meets a range of other legal criteria, including the obligation to ensure data minimalisation. If the minister approves an extension of the retention period,*

79 Dutch Parliament, Temporary Act on AIVD and MIVD investigations against countries with an offense cyber program, bulk datasets and other specific provisions (2024), https://wetten.overheid.nl/BWBR0049562/2024-07-01

80 The relevant articles from the perspective of this report are articles 14b, 14ba, 14c and 14d.

*the CTIVD reviews whether the permission has been given lawfully. The CTIVD has been granted binding powers to oversee this part of the law. These binding powers not only allow us to declare the retention of a bulk dataset unlawful, but also to order the destruction of unlawfully retained bulk datasets."*[81]

However, despite these changes, a specific legal basis for the acquisition of commercially sourced datasets is still lacking in the Netherlands. Subsuming highly sensitive datasets under the notion of "systematic open-source collection" does not satisfy the requirement of foreseeability, as it fails to clearly delineate the scope, conditions, and limits of such data acquisition.

This concern aligns with CTIVD's position expressed in a 2025 letter to parliament that certain forms of public–private cooperation continue to lack a sufficiently foreseeable legal basis accompanied by adequate safeguards.[82] As a result, the CTIVD has characterised some instances of cooperation between intelligence services and private actors in the cybersecurity domain as unlawful.

This qualification of unlawfulness should be understood in light of the structural deficiencies of the legal framework. The absence of clear and specific statutory safeguards points to a broader grey zone in which government conduct is insufficiently regulated. In such situations, the lack of foreseeability and safeguards increases the risk for unlawful interferences with fundamental rights.

Furthermore, no independent oversight mechanism exists today that is specifically tailored to data acquisition through commercial channels, including in cases involving particularly serious interferences with fundamental rights. This institutional gap reinforces concerns about both the legality and accountability of such practices.

## 5.2. United Kingdom

Another European democracy that has made significant progress addressing the challenge of intelligence agencies' access and use of commercially sourced data is the United Kingdom.

### The Investigatory Powers Act of 2016 and its shortcomings

With the Investigatory Powers Act of 2016, the UK created a statutory framework that

81 Judith Lichtenberg, Computer, Privacy and Data Protection (CPDP) conference panel on Advertisement Intelligence by European Security Agencies (2025), https://www.youtube.com/watch?v=EdTLOQGLUVI (59:00-101:00).

82 Dutch Review Committee on the Intelligence and Security Services (CTIVD), *Brief CTIVD vz TK inzake publiek-private samenwerking* (2025), https://www.ctivd.nl/site/binaries/site-content/collections/documents/2025/02/17/index/20250217_O_Brief+vz+TK+inzake+Publiek-Private-Samenwerking.pdf

contained detailed provisions governing intelligence agencies' retention and examination of bulk personal datasets (BPDs). Importantly, however, the acquisition of such datasets, regardless of the collection method used, is not subject to further restriction under this framework.[83]

An independent review of the Act in 2023 concluded that no equivalent regime exists for the retention and examination of comparable datasets when they are held by private or public institutions.[84] The Investigatory Powers Commissioner's Office (IPCO), in its annual report for 2019, had already identified a loophole that allows agencies to circumvent authorisation requirements by accessing datasets held by third parties.[85] It also noted that the access and processing of such datasets fall outside IPCO's oversight remit and recommended that this gap be addressed.[86]

The review further highlighted an additional issue concerning publicly available information for which there is a low expectation of privacy. Such datasets are currently treated in the same manner as more sensitive BPDs, despite their lower privacy implications. The report argued that the administrative burden created by this approach is disproportionate and recommended the introduction of a separate regulatory framework with less stringent safeguards for this category of data.

## New safeguards in the 2024 amendment of the IP Act

In response to the two main challenges, the existence of a loophole for highly sensitive datasets on the one side and a high administrative burden for potentially harmless datasets on the other side, the UK legislator added two new sections to the IP Act in 2024. Part 7 now includes subsections specifically addressing BPD authorisations where there is a low or no reasonable expectation of privacy. According to the UK government, accessing datasets held by commercial companies, which offer them to a broader variety of customers, "may offer the intelligence services different capabilities and insights to support them in carrying out their statutory functions."[87] The explanatory notes of the amendment bill further suggest that, in some cases, "it may be more proportionate or practical for the intelligence service to examine a dataset held by a third party rather than acquire and retain the data themselves."[88]

83 David Anderson, *Independent Review of the Investigatory Powers Act 2016* (2024), https://www.ssrn.com/abstract=4833577.
84 David Anderson, *Independent Review of the Investigatory Powers Act 2016* (2024), https://www.ssrn.com/abstract=4833577.
85 David Anderson, *Independent Review of the Investigatory Powers Act 2016* (2024), https://www.ssrn.com/abstract=4833577.
86 IPCO, *Annual Report of the Investigatory Powers Commissioner 2019* (2020), https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf.
87 UK Home Office, *Investigatory Powers (Amendment) Bill: Bulk Personal Datasets and Third Party Bulk Personal Datasets* (2024), https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-bulk-personal-datasets-and-third-party-bulk-personal-datasets.
88 UK Parliament, *Investigatory Powers (Amendment) Bill: Explanatory Notes* (2024), https://publications.parliament.uk/pa/bills/cbill/58-04/0157/en/230157en.pdf.

The two amended subsections introduce the regulatory framework for Bulk Personal Datasets (BPDs) involving either a Low or No Reasonable Expectation of Privacy (low/no BPD) or Third-Party BPDs (3PD). The first category (Part 7A) primarily addresses the systematic collection of publicly available information, commonly referred to as open source intelligence (OSINT). The second (Part 7B) governs access to commercially available data, specifically, datasets "held electronically by a third party [...] which is made available to the intelligence service as a result of arrangements with the third party, and is not generally available".

The Code of Practice underlines that this regime only applies, where the BPD remains on the system of the third party, which may be a data broker for example, and will not be obtained and retained by the intelligence service. It covers thus only what we refer to as mediated use of privately held data. If, however, the intelligence services while examining a 3PD wants to include the dataset in their own systems, they need to apply for a 'regular' BPD warrant, according to Part 7. Furthermore, in the Code of Practice the UK government sees the regime not applicable, where an "employee of a third party examines the third party's data and reports back to the intelligence service" – this, in our view, constitutes a potential loophole for circumventing the safeguards established within this regime.

**Safeguards for 3PD**

Accessing such datasets requires a warrant, applied for by the Head of the respective service, granted by the Secretary of State and reviewed by a Judicial Commissioner (with an exception allowed for urgencies). Notice, however, that these warrants can include multiple datasets at a time – including datasets that were "not available at the time of the issue of the warrant".[89] Furthermore, such warrants can also cover continuously updated datasets. Acquired databases under such warrants may, therefore, vary in terms how they interfere with fundamental rights of concerned individuals.[90] When reviewing the implementation of such warrants, it is thus crucially important, we believe, for an independent oversight body such as IPCO to ensure that a broad warrant does not undermine the thorough review of data accessed.

To mitigate these risks, the limitation of the warrant duration to twelve months is helpful. In the renewal process, the intelligence service needs to set out if it is aware of the nature of data has changed. The warrant can only be issued if the following tests are met:

89 UK Home Office, *Intelligence Services' Use of Third Party Bulk Personal Datasets. Code of Practice* (2025), https://assets.publishing.service.gov.uk/media/6841a87241cb2525c1211cf5/Intelligence_Services__use_of_Third_Party_Bulk_Personal_Datasets_Code_of_Practice_-_June_2025.pdf.

90 UK Home Office, *Intelligence Services' Use of Third Party Bulk Personal Datasets. Code of Practice* (2025), https://assets.publishing.service.gov.uk/media/6841a87241cb2525c1211cf5/Intelligence_Services__use_of_Third_Party_Bulk_Personal_Datasets_Code_of_Practice_-_June_2025.pdf.

- necessity & proportionality
- statutory purposes concerned
- interests of national security
- preventing or detecting serious crime
- interests of the economic well-being of the UK if as well relevant to the interests of national security

If the Judicial Commissioner refuses to approve of the issuing of the warrant, then the Secretary of State may refer the matter to the Investigatory Power Commissioner (IPC). If the IPC also refuses to approve the warrant, then there is no avenue of appeal for the Secretary of State.

With the amendment of the 2024, IPCO's oversight remit now explicitly covers 3PDs, as stipulated in Section 229 (3) and (9).

Interestingly, the UK government refers to the risk of undesirable outflow of information in this mode of cooperation with private actors (see also discussion in Chapter 2.3.). For instance, it is mentioned, that not all information "technically available" is as well "reasonably available" since the access to this information may have consequences for operational security.[91] In addition, there are additional safeguards for particularly sensitive material, such as information related to legally protected groups and their respective communication. While it is difficult for us to examine on whether these protection standards are high enough, from a comparative point of view it is remarkable that this extensive tiered approach is established and made accessible to the public in detail.

Regarding the oversight practice, IPCO can perform inspections on these datasets on its own initiative. To conduct such inspections, the Commissioner is granted unfettered access to the IC actors' locations, documentation and information systems. However, IPCO highlighted in their 2024 annual report the challenges of such audits. Since the data is held by third parties, it may be, according to the oversight body, "technically impossible or highly undesirable for operational security reasons".[92] Since the 7B warrants were only used from April 2025 on, IPCO has announced to report on the procedures in practice in the 2025 annual report that will be published at the end of 2026.

**Criticism**

Critical voices in the UK warned that the proposed 3PD regime could allow the services

91 UK Home Office, *Intelligence Services' Use of Third Party Bulk Personal Datasets. Code of Practice* (2025), https://assets.publishing.service.gov.uk/media/6841a87241cb2525c1211cf5/Intelligence_Services__use_of_Third_Party_Bulk_Personal_Datasets_Code_of_Practice_-_June_2025.pdf.

92 IPCO, *Annual Report of the Investigatory Powers Commissioner 2024* (2025), https://www.ipco.org.uk/publications/annual-reports/.

"to access data that has been collected or processed contrary to the law and fails to provide for the proper management of third-party BPDs"[93] . While the 3PD regime does not extend to law enforcement agencies, some British NGO fear, for example, that the "police could in some instances request access from the intelligence services to data contained in a third-party bulk personal dataset.[94]

What is more, the framework lacks sufficiently clear rules regarding the further processing and accessing of the data. For the 3PD-regime, for example, critics suggest that it needs to define under which conditions "access to a 3PD will be granted, how the intelligence services will ensure that data is not copied over to their own systems during and following examination, and how access will be terminated following the refusal, expiry, and/or non-renewal of a 3PD warrant".[95]

**Regime for low/no BPDs**

When considering applying the Part 7B regime to data that is held by third parties such as companies, the intelligence services must assess whether the data is "widely available online, whether for free or upon payment".[96] In these cases, but as well when such data is integrated in the service's own systems, the processing and retention are regulated by Part 7A. More precisely, factors that support the classification of a BPD as a low/no BPD are, when the contained data is "non-sensitive; voluntarily public or consented to; responsibly published; already in public circulation".[97] Notice, however, these factors are just indicators and much depends on the assessment of the individual case. By consequence, publicly or commercially available data used in bulk is by default covered by a stricter set of rules. To apply a lower standard, it must be assessed against these factors. This is a helpful approach to mitigate the risks of intelligence services using sensitive bulk information with little safeguards because they are considered publicly available and thus innocuous. It is also a concern raised by several oversight bodies in our research (see Chapter 4.2.)

The UK government published a Code of Practice for the implementation of the IP Act's regime for Third Party Bulk Personal Datasets. It provides examples for the different factors mentioned therein. In specific cases, such as the use of these datasets for training

93 Privacy International, and Rights & Security International, *Dangerous Data: Police Abuse of Access to Personal Data in the United States and its Global Implications* (April 2026), https://privacyinternational.org/sites/default/files/2026-04/Dangerous%20Data%20-%20RSI%20and%20PI%20-%20April%202026.pdf.

94 Privacy International, and Rights & Security International, *Dangerous Data: Police Abuse of Access to Personal Data in the United States and its Global Implications* (April 2026), https://privacyinternational.org/sites/default/files/2026-04/Dangerous%20Data%20-%20RSI%20and%20PI%20-%20April%202026.pdf.

95 Privacy International, *Privacy International's Response to the Consultation on the Investigatory Powers (Amendment) Act 2024: Codes of Practice and Notices Regulations*, https://privacyinternational.org/sites/default/files/2025-01/PI%20Consultation%20Response%20-%20IPAA%20Codes%20%28submitted%29.pdf.

96 UK Home Office, *Intelligence Services' Use of Third Party Bulk Personal Datasets (2025), https://www.gov.uk/government/publications/third-party-bulk-personal-datasets-code-of-practice/intelligence-services-use-of-third-party-bulk-personal-datasets-code-of-practice-accessible*

97 UK Investigatory Powers Act, Section 226a, https://www.legislation.gov.uk/ukpga/2016/25/section/226A.

machine learning models, the use of the data has an impact on the expectation of privacy as well. This was also underlined by IPCO in its recent annual report:

*„After careful consideration, we agree that the use to which the data will be put will be a relevant consideration, but this does not necessarily mean that the use of data for capability development and machine learning models is indicative of a low/no reasonable expectation of privacy. Depending upon the purpose of the capability or model, it might actually suggest the contrary. We will continue to keep this under review and should any category authorisation be submitted in this area it will need to satisfy a Judicial Commissioner that it has appropriate parameters."*[98]

If an information of particular sensitivity is discovered within the dataset after the authorisation, either the whole dataset needs to be deleted, the information of concern needs to be isolated and deleted or the whole dataset needs to be authorised as a standard BPD according to the regime in Part 7. Every authorisation under Part 7A needs to be renewed after twelve months, but the intelligence services are held to regularly evaluate the continued operational and legal justification of the retention. The frequency of the review depends on the precise case but should happen at least once before the end of the 12-month period.[99]

For the IPC to be able to inspect the data retention and processing under this regime, the intelligence services are required to keep all applications and authorisation records as well as granular statics on different features of the authorisation processes. Furthermore, the IPC must be granted full and unrestricted access to all locations, documentation and information systems.

Authorisation for the acquisition of low/no BPDs is granted by the Head of the intelligence services or a person on their behalf and approved by Judicial Commissioner – unless the retention is covered by an existing broader category authorisation.

| Dataset | Definition | Safeguards | Authorisation Process |
|---|---|---|---|
| Bulk Personal Datasets (BPDs) – Part 7 | Large datasets retained and examined by intelligence services, containing personal data where most individuals are not of intelligence interest. | • Retention and examination of data require a BPD warrant<br>• Application must include sensitive data | Secretary of State issues the warrant, Judicial Commissioner approves (Double Lock) |

98 IPCO, *Annual Report of the Investigatory Powers Commissioner 2024* (2025), https://www.ipco.org.uk/publications/annual-reports/.
99 UK Home Office, *Intelligence Services' Use of Third Party Bulk Personal Datasets (2025).* https://www.gov.uk/government/publications/third-party-bulk-personal-datasets-code-of-practice/intelligence-services-use-of-third-party-bulk-personal-datasets-code-of-practice-accessible.

| | | | |
|---|---|---|---|
| | | indicators<br>• Warrant period used to be 6 months (after 2024 amendment: 12 months), can be renewed | |
| Part 7A on BPDs with Low or No Reasonable Expectation of Privacy | Datasets where individuals have a low or no reasonable expectation of privacy, including publicly or commercially sourced information. | • Safeguards are less onerous on IC than Part 7 safeguards due to reduced privacy expectations | Head of IC actor authorises, Judicial Commissioner approves (unless urgent).[100] |
| Part 7B on Third Party Bulk Personal Datasets (3PDs) | Datasets held electronically by third parties (e.g., government departments or commercial entities), accessed by intelligence services in situ without retention. | • Requires a 3PD warrant to examine data (unless other authorisation scheme applies)<br>• Application includes sensitive data indicators<br>• Secretary of State must approve criteria for handling legally privileged data<br>• IPCO informed if such data retained<br>• Sanctions for offences related to unlawful access defined in statutory law (up to two years imprisonment) | Head of Intelligence Services applies for the warrant, Secretary of State issues the warrant; Judicial Commissioner reviews necessity/proportionality and IPCO can review refusals |

**Criticism**

The approach followed by this regime remains contested. Several civil society actors in the UK argue that this regime with low safeguards creates a high risk for unchallenged fundamental rights infringements. They argue that even seemingly innocuous data can reveal highly sensitive information. This risk is further increased by the rapidly evolving technical capabilities, in particular machine learning techniques.[101]

Furthermore, given the opaque and complex practices of data aggregation by brokers,[102] it should not be readily assumed that people consented to government access of data held by private sector entities. Byron Tau, an investigative journalist, has made this point in response to similar arguments made by the U.S. government:

*"The truth is that no consumer or citizen can know what data is being collected about them or how it's used, let alone consent. To say that anyone has consented to live in this world is a lie, because there is no way for the average consumer to even begin to understand the flow of data from their consumer technologies to corporate America and then to the security services of nearly every powerful nation on earth."*[103]

In sum, the UK now features two new chapters in its amended IP Act that deal with commercially sourced data when used in bulk form, which, arguably, is the default case for most forms of data acquisition and processing by modern intelligence agencies. Bulk datasets with a privacy expectation and which are being integrated into the IT systems of the services (i.e. "sovereign data use") are covered in Chapter 7 of the IP Act. If bulk datasets are held by third parties, e.g. data analytics and surveillance entrepreneurs in the private sector, then the responsibilities for the UK government's involvement are covered in the newly created Part 7B of that chapter within the IP Act. The 2024 reform also introduced another regime, namely Part 7A for data that the UKIC integrates into its own systems but for which there is no/low expectation of privacy. Notice, though, that these new rules cover thus far only the processing and retention of such data. By contrast, the new legal regime does not include yet any guidance for the services and the public alike as concerns the acquisition of such data.

## 5.3. United States of America

To its credit, the U.S., unlike many democracies across the world, has produced a document with publicly available information on how its intelligence agencies access and use commercially sourced data. Since 2024, the interested public can consult the *ODNI*

100 Section 226BB of the IP Act, https://www.legislation.gov.uk/ukpga/2016/25/section/226BB.
101 Internet Society, *Investigatory Powers (Amendment) Act 2024: Consultation Response to the Home Office* (2025), https://www.internetsociety.org/resources/doc/2025/investigatory-powers-amendment-act-2024-consultation-response-to-the-home-office/.
102 Privacy International, *PI's Response to the UK Government's Investigatory Powers (Amendment) Bill* (2024), https://privacyinternational.org/advocacy/5258/pis-response-uk-governments-investigatory-powers-amendment-bill#:~:text=We%20responded%20to%20both%20consultations,privacy%20and%20sec
103 Byron Tau, *Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State* (2024), https://www.penguinrandomhouse.com/books/706321/means-of-control-by-byron-tau/.

*Policy Framework for Commercially Available Information*.[104] Also in 2024, former U.S. President Biden issued Executive Order 14117 which contained important standards and restrictions intended to "preventing access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern".[105]

We will concentrate on the ODNI Policy Framework here. It contains several detailed rules, procedural guidelines and obligations that regulate the acquisition, access, use, transfer and deletion of commercially sourced data by IC actors and PSEs acting on their behalf.[106] The document also refers to additional set of regulations some of which are also publicly available. The rules and standards expressed in the ODNI Policy Framework not only inform the public but are also legally binding for the intelligence agencies.

At the outset, it needs to be said, however, that the U.S. has not placed these important set of rules on a statutory footing. The U.S. Congress, in other words, was not involved in the adoption of these rules. Rather, the ODNI Policy Framework is a document by the executive branch of government that features key standards and rules that govern internal IC processes regarding (sensitive) commercially available information. Thus, the framework not only lacks democratic legitimacy, but it also omits provisions on the responsibilities of institutions outside of the executive branch of government to authorise, verify, review, oversee and account for government conduct in this field. Granted this may not be expected from a document drafted by the executive branch for the executive branch, but - to date - the U.S. lacks additional binding regulations passed by both Houses of the U.S. Congress.[107] Unlike laws passed by the U.S. Congress, government policy frameworks, executive orders or -decrees offer less assurance and stability for the general public, the IC and its international partners: the President of the U.S. can rescind or replace such documents far more easily.[108] Crucially, U.S. courts do not have jurisdiction to enforce executive orders.

Having noted these important shortcomings, the ODNI Policy Framework is part of the U.S. national legal framework on intelligence collection. As such, the ODNI Policy Framework for Commercially Available Information is a key reference document that

104 ODNI, *Intelligence Community Policy Framework for Commercially Available Information.*

105 See Executive Office of the President, *Executive Order 14117: Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (28 February 2024), https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

106 See relevant excerpts from the ODNI Policy Framework added in the text boxes in the Annex.

107 The Fourth Amendment Is Not For Sale Act, has not become law for it then stalled in the U.S. Senate. Unlike the ODNI Policy Framework, the Fourth Amendment is Not for Sale Act had foreseen to "*prohibit* intelligence and law enforcement agencies from purchasing certain sensitive information about U.S. persons from third-party sellers, including geolocation information, communications-related information, and information obtained through illegitimate scraping practices. Similarly, another unsuccessful legislative attempt, the Government Surveillance Reform Act, would have *barred* intelligence and law enforcement agencies from purchasing an even wider swath of U.S. person data, with exceptions to allow “overcollection” - combined with rigorous minimization requirements - in cases where the government cannot identify and/or remove U.S. person information before acquiring datasets." In Ayoub, Emile, *Assessing the Intelligence Community’s Policy Framework for Commercially Available Information* (2024), https://www.justsecurity.org/96015/commercially-available-information/.

108 National Resource Governance Institute, *Legal Framework: Navigating the Web of Laws and Contracts Governing Extractive Industries* (2015), https://resourcegovernance.org/sites/default/files/nrgi_Legal-Framework.pdf, p. 1.

provides guidance on standards applicable to "the IC's access to and collection and processing of certain sensitive forms of CAI".[109] The document directs all "IC elements to adopt this Policy Framework" and "dedicated IC officials, including privacy and civil liberties, oversight, compliance, and legal officers, provide counsel and monitor compliance with these laws and policies".[110] The ODNI also needs to report to Congress and separately to the general public on the implementation of the policy framework and its potential need for adjustment.

As a policy framework drafted by the executive branch for the executive branch, the ODNI Policy Framework U.S. "does not prohibit IC elements from purchasing data that otherwise would require a warrant, court order, or subpoena to obtain."[111] This has led many observers to cast doubt on the usefulness of these rules. Many civil society organisations caution that an executive-level policy framework is not sufficient. Rather, they call for congressional action to close the data broker loophole, among other objectives. Apart from calls for congressional action and additional questions whether some types of commercially sourced data should be procured and processed in the first place, the question arises whether the standards and rules of the ODNI policy framework are satisfactory in their own right. Some observers caution that "its subjective, discretionary, and exception-riddled standards risk making this framework a box-checking exercise for agencies"[112] and that the U.S. IC should not be "permitted to replace the judgment of Congress and the courts with its own balancing test."[113]

## 5.4. Germany

Whereas policymakers and oversight bodies in the UK, the Netherlands and the United States have either adjusted their national legal frameworks and corresponding oversight practice or at least publicly recognised the need to better govern the fast-evolving and multi-facetted cooperation between the intelligence services and private companies, German stakeholders have yet to confront this momentous challenge.

While the UK, U.S. and Dutch governments acknowledged their use of commercially sourced data which they access or obtain through means other than a legal obligation (compelled access), the German government is more reluctant to address this in public. The legislator, by contrast, is only gradually becoming aware of the issue. The public debate on the legality of their government's access and use of CSD, spurred by investigative journalists reporting on the matter, has begun, however.

109 ODNI, *IC Policy Framework for Commercially Available Information* (2024).

110 Ibid, p.1-2.

111 Emile Ayoub, *Assessing the Intelligence Community's Policy Framework for Commercially Available Information* (2024), https://www.justsecurity.org/96015/commercially-available-information/.

112 Ibid.

113 Ibid.

Interestingly, the German government itself contributed to this by means of a revealing clarification in an explanatory text on an amended legal provision regarding the transfer of publicly available information: The document clarified that it "*also applies to the transfer of data obtained through the purchase of, for example, extensive advertising databases and other databases with a comparable level of intrusiveness".*[114]

A recent *research paper* by the Parliamentary Research Service[115] of the Bundestag sheds further public light on the matter.[116] Its neutral and matter-of-fact analysis exposes ambiguity and severe gaps in the current German legal framework with regard to the necessary protections for interferences with fundamental rights that could arise from the purchase of personal data from commercial advertising database by German intelligence services. The paper reminds readers that "no reliable information is currently available on the actual frequency and scope of purchases of such data by German government agencies" only to caution that there are "indications that suggest that this practice is not an exceptional phenomenon, but is increasingly becoming part of official information management."[117] The paper then establishes that such purchases by German intelligence services would constitute an interference with the fundamental right to the privacy of telecommunications[118] and informational self-determination.[119]

By consequence, the paper argues, were these *indications* of data purchases to materialise (as happened recently regarding another EU Member State),[120] then this would urgently require a sufficient statutory basis to justify such profound interferences with these fundamental rights. Interestingly, the Research Service then makes three detailed attempts – but fails each time – to identify a norm in the current legal framework on intelligence collection that would unequivocally meet the high standards set forth by the German Constitutional Court.

In a nutshell, the Research Service was unable to identify without reservations a sufficient statutory basis for intelligence services' data purchases from commercial vendors. The document features strong arguments why the nearest suitable current provisions in the German intelligence law framework would still likely fail the required constitutional standards of specificity and proportionality. For example, the Research Service finds that

114 Bundesregierung, *Entwurf eines Gesetzes zur Änderung des BND-Gesetzes, Drucksache 20/8627 (2023),* pages 42-43, https://dserver.bundestag.de/btd/20/086/2008627.pdf

115 The Research Service of the Bundestag is a non-partisan research unit within the German parliament that provides independent analyses to MPs on legal, political, and social issues to support informed decision-making.

116 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

117 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

118 Article 10 of the German Constitution.

119 Article 2(1) in conjunction with Article 1(1) of the German Constitution.

120 Szabolcs Panyi, 'Orbán's Spying Kit Revealed: Israeli Surveillance Tool Combined with Hungarian Technology', 09 April 2026, https://vsquare.org/orban-spying-toolkit-cobwebs-webloc-hungary-spyware-citizen-lab/.

- “data stored in commercial databases” usually originates “from numerous different sources, many of which are not generally accessible“[121] ;
- “the fact that the operators of advertising databases sell and disclose the data voluntarily does not, incidentally, change the intrusive nature of the purchases, as they themselves were not involved in the communication process from which the traded data originated.“[122]

The analysis is also insightful in as much as it recalls the various material requirements, specifications, and procedural steps such as an independent approval procedure and administrative control of data processing that apply to surveillance methods of intelligence agencies that interfere profoundly with fundamental rights.[123] It also clarifies that such requirements "do not apply to operators of commercial databases. The circumstances and methods under which the data is collected and entered into the database are therefore completely open and cannot be verified with sufficient certainty by the purchasing intelligence service."[124] Moreover, the paper recalls that surveillance measures which profoundly interfere with fundamental rights need to be “suitable, necessary, and proportionate for achieving a legitimate aim.”[125]

In the context of intelligence agencies purchasing data, the Research Service cautions “proportionality in the strict sense may be particularly problematic”.[126] Given that there are legitimate doubts “as to whether the data offered by commercial vendors are accurate at all”[127] and the “possibility that the data were collected unlawfully,”[128] it must be taken into account that this, in turn, could “significantly increase the intensity of the interference with the fundamental rights of those concerned associated with an intelligence data purchase.”[129] Ultimately, “these considerations may carry such weight in the balancing exercise against the objective pursued that, in this case, the purchase

121 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

122 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

123 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

124 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

125 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

126 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

127 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

128 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

129 Wissenschaftliche Dienste des Deutschen Bundestages, *Rechtliche Voraussetzungen und Grenzen des Behördlichen Ankaufs von Personenbezogenen Daten aus Werbedatenbanken* (2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf (LLM-based translation).

would not be proportionate and therefore impermissible."[130]

Summing up, there is no provision in the current German legal framework that could serve as suitable statutory legal basis for the acquisition, processing and retention of commercially sourced data by the German intelligence services.[131] The only aspect that is at least partially covered is the sharing of information from commercially sourced datasets.[132] While the risks to fundamental rights are profound in the data sharing context, the German parliament ought to introduce safeguards also for the other phases in the lifecycle of government interaction with commercially sourced datasets. At present, there are no tangible limitations on the intelligence services' acquisition of commercial advertising databases and there are also no specific requirements governing the lawful processing of the data thus obtained. In addition, there are no concrete review standards written into the formal mandate of independent oversight bodies for such practices. All of this would be necessary, however, in order to legitimise the potentially large-scale interferences with fundamental rights that may result from intelligence data purchases.

There is, therefore, an urgent need for legislative action in Germany. Addressing and closing this accountability gap would serve not only the interest of legal clarity for staff within the security authorities, but also the rule of law and the protection of fundamental rights. Introducing new reporting obligations for oversight bodies would also enhance public knowledge about this important field of contemporary intelligence practice.

To this day, sadly, no German oversight body has explicitly addressed this issue in public either. In the latest annual report of the Federal Data Protection Commissioner (BfDI) referred to a not further specified case where:

*"the BND processes large volumes of data without there being a sound legal basis for it that is, in light of the parliamentary reservation, free from doubt. These processing activities also affect a large number of German citizens."*[133]

We think that it is very likely that this refers to commercially sourced dataset – which would be highly problematic, given the insufficient legal framework in Germany.

130 Wissenschaftliche Dienste, *Rechtliche Voraussetzungen Und Grenzen Des Behördlichen Ankaufs von Personenbezogenen Daten Aus Werbedatenbanken*, 17.

131 Svenja Efinger and Thorsten Wetzling, *Wanted: A legal authority for data purchases by German security and intelligence agencies* (2026), https://aboutintel.eu/commercial-data-adint-germany-intelligence-reform/.

132 Deutscher Bundestag, *Deutscher Bundestag - Bundestag Novelliert Die Rechtsgrundlagen Der Nachrichtendienste* (2023), https://www.bundestag.de/dokumente/textarchiv/2023/kw46-de-bnd-976564.

133 Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Tätigkeitsbericht 2025 – 34. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit* (2026), https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/34.TB/34TB_25.html, LLM-translated.

## 5.5. Summary

This chapter has compared the national legal frameworks of four democracies with a view to their ability to regulate and restrict the intelligence agencies' increasing acquisition and use of commercially sourced data.

Government and independent oversight bodies in the Netherlands and the United Kingdom have publicly acknowledged that the paradigm shift in intelligence services' work is insufficiently reflected in the IP Act of 2016 and the Wiv 2017, respectively. While the large datasets held by private companies form an increasingly important asset for intelligence services, these older legal frameworks were not able to provide sufficient guidance to help ensure that the services act lawfully.

**The Dutch legislator** has addressed one issue that was criticised by the independent oversight body CTIVD with the help of a temporary regulation that provides a framework for the *processing* and *retention* of bulk datasets, regardless of how they were acquired. Thus, it covers commercially sourced data, too. It remains to be seen, however, how this will be integrated in the upcoming reform of intelligence legislation. An issue, criticised by the independent oversight body as well, is the lacking statutory specific legal basis for the *acquisition* of commercially sourced data has not been addressed, yet.

The **United Kingdom** has integrated a similar framework in its 2024 amendment of the Investigatory Powers Act. It now includes two new legal regimes that cover the processing and retention of bulk datasets held by third parties, including private companies, and datasets with low expectation of privacy. The later relates mostly to OSINT data. Furthermore, the independent ex-ante oversight as well as the ex-post audit were strengthened, and some gaps were filled. However, there is still no specific statutory basis for the *acquisition* of commercially sourced data itself.

That said, both democracies follow a useful tiered approach to capture the sheer multitude of different modalities in public-private cooperation on commercially sourced data. In both cases the sensitivity of the data contained in the datasets is the decisive factor. Both democracies feature rigorous independent ex-ante oversight for sensitive datasets.

The **United States** has, to its credit, introduced publicly available guidance on intelligence agencies' access to commercially sourced data, notably through the 2024 ODNI Policy Framework. It establishes binding rules for the acquisition and use of such data, alongside internal compliance and reporting obligations. As an executive branch instrument, however, it lacks democratic legitimacy. It also can be changed or revoked more easily. It also does not prohibit the purchase of data that would otherwise require legal authorisation. Its discretionary standards are deemed insufficient, therefore, and congressional action is needed to close existing loopholes.

In **Germany**, the situation is markedly different, however. Aside from adopting data-sharing provisions in 2023 that apply also to commercially sourced data, the legislator has not yet woken up to the ADINT challenge. To date, there is neither a sufficiently clear legal basis for the intelligence agencies' acquisition or commercially sourced data nor does the current German legal framework on intelligence included sufficient rules governing its processing and retention.

This chapter has also noted how, in the United Kingdom and the Netherlands, oversight bodies have proactively identified and addressed shortcomings in both the legal framework and oversight practices. In Germany, by contrast, there has been no reporting yet by the independent oversight bodies on the specific issue of the intelligence services' access and use of commercially sourced data. Consequently, the public remains largely uninformed about how intelligence services engage with the data industry – and how such engagement may interfere with fundamental rights.

Given the vast amount of personal data available on virtually every individual in different spheres from public to private actors, a holistic approach to the accessing and processing of large datasets is now an increasingly pressing matter that lawmakers and oversight bodies need to address across several jurisdictions. The following chapter offers several recommendations that may be helpful for it.

---

# 6. Good practice and policy recommendations

The multifaceted collaboration between intelligence agencies and private actors in the context of commercially sourced data entails risks both for the provision of national security and the protection of fundamental rights. Empirical results from our oversight practitioner survey (see Chapter 4) and insights into the evolution of legal frameworks in four democracies (see Chapter 5) show that our democracies are, at best, waking up to the ADINT challenge. Apart from a lack of knowledge among regulators and proactive reviews and audits among oversight bodies, there are also too many gaps and too much legal ambiguity in the national legal frameworks on intelligence collection to prevent disproportionate government access to data.

Hoping to contribute to positive change, this chapter now presents good practice examples from different jurisdictions. It also addresses a series of recommendations to lawmakers, policymakers, oversight bodies and the intelligence and security services. Granted, updating the current legal framework and oversight practice is ambitious. It takes a village to earn and maintain democratic legitimacy and public trust for national security governance that interferes with fundamental rights.

The following recommendations are presented in different sections depending on whether they address the legal frameworks on intelligence collection (Section 6.1.), the formal mandate of oversight institutions (Section 6.2.), the practices of intelligence services (Section 6.3.) and the practice of oversight bodies (Section 6.4.). Where possible, we signify whether a particular aspect pertains to a different phase in the lifecycle of commercially sourced data use by the intelligence agencies.

The recommendations are not meant to be exhaustive. We invite constructive feedback and welcome further good practice examples.

## 6.1. On the legal framework regulating intelligence services' activities

We recommend the adoption of a standardised legal framework to govern government conduct and responsibilities in this space. Without it, it will become increasingly difficult to govern and harmonise the multitude of data exchanges and payments that are potentially taking place in this space. Such a comprehensive new legal regime on the use of commercially sourced data by intelligence services structures and guides the necessary oversight activities, too.

For this,

- it should provide **clear definitions** that distinguish publicly available information from commercially available information;
- it should include **new warrant requirements** so that existing requirements for warrants to obtain similar data can no longer be circumvented. For example, if federal U.S. law enforcement agencies were obliged to obtain warrants before collecting cell site location information for over seven days and other government agencies could simply purchase comparable data from commercial vendors and then share that data with the federal law enforcement agencies, then this would defy the purpose of the initial warrant requirement;
- it should require that the heads of the agencies (or designated personnel) **provide written justification in warrant applications** before they can acquire commercial data, including obligations to document the number and types of commercially sourced data to be procured, as well as the associated costs;
- it should regulate **the procurement of CSDprior to the conclusion of contracts**, particularly in cases involving the testing of new technologies in cooperation with private companies.

**Good Practice:**

- In **the Netherlands**, prior to accessing a dataset, services are obliged to prepare an *acquisition memorandum* assessing the necessity, proportionality, and subsidiarity of the acquisition. This mechanism operationalises the requirement for written justification prior to data procurement and offers a replicable model for other jurisdictions seeking to regulate the pre-access phase.

- In the **United Kingdom**, when accessing certain types of commercially sourced data in the UK, the intelligence agency must obtain a *warrant* issued by the Secretary of State and approved by a Judicial Commissioner. In instances where there is a low expectation of privacy, authorisation may be granted by the head of the IC entity or a designated individual. Judicial Commissioner approval is still required, except in urgent circumstances, where the examination needs to be done post-facto.

A new or amended legal framework should also

- address the practice of mediated data access more thoroughly also with a view to **prevent the circumvention of data minimisation requirements** that commonly exist for bulk data;
- require an **inventory of databases** - both for those that the intelligence agencies use on their own IT systems and for those to which they only have mediated access through PSEs;
- create a **distinct legal basis for mediated data access**, e.g. when intelligence agencies access data stored on private servers.

**Good practice:**

- The European Union's General Data Protection Regulation (GDPR) contains several important provisions on the access and use of personal data that would help to reduce disproportionate government conduct in this field. However, national security agencies are largely exempt from this regulatory framework. In this context, we note that **Belgium's Data Protection Act** and its 2024 amendment provide for the national implementation of the GDPR provisions and contains provisions specifically addressing intelligence and security services. [134]
- Many Member States of the Council of Europe signed and ratified the **Modernised Convention 108**. This document includes important provisions on the processing of personal data which also apply the field of national security and defence.

  **Caution** is advised, however, as the scope of its exceptions and restrictions regime (Article 11) is currently determined among Member States. [135]

**Food for thought:**

- Should the rules for the intelligence agencies' access and use of data depend on the source of the data or on the potential insights that can be derived from the dataset? We think that the latter approach may be preferable since the severity of the impact on fundamental rights from accessing and processing a dataset depends more on what the data can reveal than on how it was obtained. Should lawmakers opt for this approach, however, they need to be clear on what criteria they should use to evaluate the impact on fundamental rights, and which actors should be involved in this assessment at what stage in the lifecycle of commercially sourced data. A comprehensive approach on regulating the processing of datasets also reduces the risk of loopholes in the legal

134 See Data Protection Laws in Belgium. https://www.dlapiperdataprotection.com/index.html?t=law&c=BE.

135 For an introduction into this, see: Thorsten Wetzling and Charlotte Dietrich, Report on the need for a Guidance note on Article 11 of the modernised Convention 108, June 2021, https://rm.coe.int/t-pd-2021-6-draft-guidance-note-on-exceptions-under-article-11-of-the-/1680a2d512

regime. Additionally, a holistic approach would promote a more technology-neutral and future-proof legal regime. This said, a national legal framework also needs to be specific enough to provide a foreseeable legal basis and guidance to oversight bodies.

**Good practice:**

- Following repeated scrutiny and recommendations by the Norwegian EOS Committee, the **Norwegian government** changed its position and now considers the individual procurements of data from commercial providers as an intrusive method under Chapter 6-2 of the Norwegian Intelligence Service Act.[136]

**Caution**:

- The relevance of this new approach depends on the density of Norwegian regulations that guide the collection of openly available information.[137]
- Does this apply only to nationals?[138] In our interconnected world, nations should strive to increase the rights for non-nationals, too

When it comes to **data processing,** the legal framework should

- oblige intelligence agencies to **define queries** and to appoint designated and trained employees to ensure compliance with data processing and documentation requirements;
- **cover non-content data**, such as meta-data of communication or other sensitive information to reflect the potential sensitivity of this kind of information;
- oblige intelligence services to thoroughly **document** the purpose and mechanisms of their data collection as well as subsequent processing;
- require that **log recordings** have to be made available to oversight bodies for the purpose of their audits;
- require that if **significant changes** are made to bulk datasets that such changes be detailed in an **application to renew the authorisation**.

**Good Practice:**

- In the **United Kingdom,** the legal framework that applies also in part to processing commercially sourced data includes individual sanctions for deliberate misconduct, with penalties that can include up to two years of imprisonment.[139]
- In **the Netherlands** bulk dataset is reassessed against the requirements of necessity,

136 EOS Committee, *Annual Report 2024* (2025), Section 4.9, https://eos-utvalget.no/wp-content/uploads/2025/06/EOS-annual-report-2024.pdf

137 This is because, as per EOS Committee report, the new position is that "as a rule, purchasing information from commercial enterprises constitutes collection of openly available information pursuant to the Intelligence Service Act Section 6-2." We note here that the *systematic* collection of openly available data needs a wide range of safeguards as seemingly innocuous information can interfere gravely with fundamental rights, especially if this data is collected in enormous troves and triangulated with other data to which the intelligence services may have access.

138 The EOS Committee report stated in this regard also: "The territorial prohibition therefore applies to such purchases." EOS Committee, *Annual Report 2024* (2025), https://eos-utvalget.no/wp-content/uploads/2025/06/EOS-annual-report-2024.pdf

139 See UK IP Act, Section 226ID, https://www.legislation.gov.uk/ukpga/2016/25/section/226ID.

proportionality and subsidiarity when there have been substantial changes to the dataset. If the reassessment leads to the conclusion that a different access regime should apply to the bulk dataset, a proposal to that effect will be submitted to the responsible minister.[140]

- In **Canada**, a designated employee must evaluate any bulk dataset within 90 days from the date it is collected. During this evaluation, the employee is responsible for deleting any personal information that is not relevant to the mandate of the IC entity. During this period extraneous, erroneous, or low quality data may be removed, and translations or decryption conducted.[141]

When it comes to **data deletion,** lawmakers should bear in mind that

- record-keeping obligations usually require the retention of at least some residual data.

**Good Practice:**

- In the **Netherlands**, bulk datasets obtained through special powers must be destroyed after 18 months. Exceptionally, the services can request permission from the relevant minister to retain a bulk dataset for an additional 12 months if there is an urgent need to do so for national security purposes. To get a permission, the services must demonstrate that such a retention is necessary and proportionate and it meets a range of other legal criteria, including the obligation to ensure data minimalization. If the minister approves an extension of the retention period, the CTIVD reviews whether the permission has been given lawfully. The CTIVD has been granted binding powers to oversee this part of the law. These binding powers enable CTIVD not just to declare the retention of a bulk dataset unlawful, but also to order the destruction of unlawfully retained bulk datasets.
- In the **United Kingdom**, if a dataset contains information that is subject to legal privilege (e.g. the protected communication of lawyers with their clients), individuals within the intelligence community are obliged to inform the Investigatory Powers Commissioner (IPC). The IPC must then direct that the data is destroyed or impose condition to the use or retention. This does not hold if the public interest in retaining the data is stronger than its deletion or retaining is necessary for interests of national security or preventing death or significant injury.[142]

When it comes to **data sharing,** the legal framework should

define under which conditions which type of commercially sourced data can be shared with which agencies or third parties to mitigate the risk of circumventing rules on purpose limitation.

140 Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017, article 3, https://wetten.overheid.nl/BWBR0044304/2020-11-06.
141 National Security and Intelligence Review Agency, *Review of CSIS Dataset Regime* (2024), https://publications.gc.ca/collections/collection_2024/ossnr-nsira/PS108-6-2024-eng.pdf
142 UK Home Office, *Intelligence Services' Use of Third Party Bulk Personal Datasets. Code of Practice (2025)*, https://www.gov.uk/government/publications/intelligence-services-retention-and-use-of-bulk-personal-datasets/intelligence-services-retention-and-use-of-bulk-personal-datasets-code-of-practice-accessible.

**Good Practice:**

- In **Germany**, the national legal framework for intelligence uses a nuanced approach to governing data sharing. It distinguishes between different categories of actors including national intelligence services, law enforcement agencies, private entities, international partners and intergovernmental organizations. Distinct rules apply to each category of actors. This framework also extends to commercially sourced information when it is collected systematically.[143]

## 6.2. On the legal mandate of oversight bodies

When it comes to the legal mandate of oversight bodies, we recommend lawmakers to

- grant **full access for oversight bodies** to all data storage locations, documentations and information systems;
- grant oversight bodies access to **comprehensive log recordings** of processed CSD and adequate tools to analyse log-files;
- establish a more prominent role for **independent data protection officers** in overseeing intelligence services' data purchases;
- empower oversight bodies to **compel PSEs** to help with their investigations and audits;
- expand the formal remit of oversight bodies to also include the possibility to sanction the non-adherence to its recommendations.

**Good Practice:**

- In **Norway**, the EOS-Committee can extend its review focus to private sector organisations that work for or with the security and intelligence sector. If the EOS-Committee learns that a service uses information provided by a private actor, it can compel access to the information it needs for its investigation *directly from the private sector entity.*

## 6.3. On the practice of governments and intelligence services

For national security reasons, governments should ensure that they adopt a common information security and auditing framework for private sector entities (PSEs) when they access or use their datasets. Intelligence actors must make constant and rigorous effort to inquire about the contents and quality of information contained in commercially sourced datasets.

143 German BND Act, Art. 10a and p.42f of the explanatory notes of the 2023 reform of the law, https://dserver.bundestag.de/btd/20/086/2008627.pdf.

Governments should also find ways to ensure that the same data is not purchased multiple times by different entities at different costs. Harmonised standards are also recommended in the interest of data security and cyber security.

**Good Practice:**

- In the **United States**, the ODNI's Intelligence Community Policy Framework for Commercially Available Information contains numerous helpful provisions on how to mitigate bias in data access, data integrity and special approvals for accessing sensitive commercially available data (to mention a few examples).
- In the **United States,** the Privacy and Civil Liberties Oversight Board (PCLOB) recommends in its report on the National Counterterrorism Center (NCTC) that it should "apply a comprehensive compliance framework that addresses information security risks and auditing requirements for commercial vendors that own or control datasets that NCTC analysts access via the access paradigm. Such a framework should address training requirements, user behaviour agreements, encryption requirements, incident response procedures, audit requirements, and other elements typically required by an information security program. This framework should be agreed to contractually between NCTC and each commercial vendor who owns or controls the relevant datasets, to ensure commercial vendors are providing appropriate protections."[144]

When it comes to the processing of information, governments should

- publish implementation guidelines for rules pertaining to the agencies' use of commercially sourced data.

**Good practice:**

- In the **United Kingdom**, the government has published a detailed code of practice on the intelligence services' use of third party bulk datasets.[145]
- In **Canada**, a designated employee must evaluate any bulk dataset within 90 days from the date it is collected. During this evaluation, the employee is responsible for deleting any personal information that is not relevant to the mandate of the intelligence agency. During this period extraneous, erroneous, or low quality data may be removed, and translations or decryption conducted.[146]
- In the **Netherlands**, a bulk dataset is reassessed against the requirements of necessity, proportionality and subsidiarity when there have been substantial changes to the dataset. If the reassessment leads to the conclusion that a different access regime should apply to the bulk dataset, a proposal to that effect will be submitted to the responsible minister.[147]

144 Privacy and Civil Liberties Oversight Board, *Report on the National Counterterrorism Center* (2024), https://documents.pclob.gov/prod/Documents/OversightReport/4ce093a4-d28d-4996-a35b-c11d18e19018/PCLOB%20FY2024%20NCTC%20REPORT%20-%20Completed%20508%20-%20Dec%2017%202024.pdf.

145 UK Home Office, *Intelligence Services Use of Third Party Bulk Personal Datasets - Code of Practice* (2025), https://assets.publishing.service.gov.uk/media/6841a87241cb2525c1211cf5/Intelligence_Services__use_of_Third_Party_Bulk_Personal_Datasets_Code_of_Practice_-_June_2025.pdf

146 National Security and Intelligence Review Agency, *Review of CSIS Dataset Regime* (2024), https://publications.gc.ca/collections/collection_2024/ossnr-nsira/PS108-6-2024-eng.pdf

147 *Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017*, Article 3.

- In the **United Kingdom**, "it would be an offence, subject to a maximum sentence of two years, to examine data in a third-party BPD, knowing or believing that it was not necessary and proportionate."[148]

When it comes to **reporting**,

- agencies should report regularly to their political masters, to the oversight bodies and also to the general public.

**Good Practice:**

- In the **United States**, as per the ODNI's Policy Framework, the intelligence community needs to report to the Director of National Intelligence, to Congress and every two years to the public.

**Good recommendation:**

- According to the **Canadian** review body NSIRA, the Canadian intelligence agency CSIS should analyse and document any reasonable expectation of privacy when assessing datasets that are considered publicly available. It also recommends further training to its employees to enable them to apply the correct legal basis.[149]

## 6.4. On the practice of intelligence oversight bodies

Oversight bodies can proactively shape the governance of the intelligence agencies' access to commercially sourced data even if the pertinent legal framework provides no explicit remit to review this nascent field of intelligence.

**Good Practice:**

- In **Denmark**, the TET oversight body regularly conduct structured and mythologically very rigorous risk assessments which may then lead to a shift in priorities and the right allocation of resources.[150]

148 House of Commons, *Research Briefing on Investigatory Powers Amendment Bill* (2024), https://researchbriefings.files.parliament.uk/documents/CBP-9960/CBP-9960.pdf; and its statutory footing in Section 226ID "Offence of breaching safeguards relating to examination of material" of the IP Act.

149 National Security and Intelligence Review Agency, *Review of CSIS Dataset Regime* (2024), https://publications.gc.ca/collections/collection_2024/ossnr-nsira/PS108-6-2024-eng.pdf

150 Danish Intelligence Oversight Board, *Standards for Danish intelligence review activities* (2024) https://tet.dk/wp-content/uploads/2025/04/TET_Standard_2024_UK.pdf

Going forward, we recommend that national intelligence oversight bodies should

- reach out more proactively to the national bodies overseeing the processing of data in the private sector and identify ways in which they could potentially help each other;
- where possible, seek to obtain a better overview of accessible log files to see when data may be transferred to private actors;
- find ways to be involved in data procurement decisions which would allow them to contribute to the development of adequate tools for log-file review;
- test if limited time and personnel resources may be meaningfully and securely compensated through the responsible use of AI tools, e.g. to review contracts between intelligence services and private actors prior to their conclusion.

**Good practice:**

- In **the Netherlands,** the independent oversight body CTIVD systematically assessed if in the acquisition notes the correct legal basis was referred to and if necessity and proportionality of the acquisition were sufficiently substantiated.[151]
- In **the Netherlands,** the CTIVD has recommended already back in 2017 that internal policies should be adjusted "in such a way that it becomes clear when which legal basis (open source, informant or agent) applies when acquiring bulk datasets offered by third parties on the Internet."[152] This recommendation was implemented and has significantly improved the situation, whereas there were previously systematic problems with the application of the correct legal basis, a follow-up report in 2024 described this issue as reduced to isolated incidents.[153]
- In **the Netherlands**, the CTIVD demanded in a public report that the Dutch services should increase their data minimisation efforts and that the possibility of data minimisation should be part of the proportionality test before acquiring or further processing a bulk dataset.[154]

### When it comes to the review of CSD processing, oversight bodies should

- regularly review log recordings and demand more granular information if shared information is not sufficient;
- examine whether datasets that were once approved by a warrant still work in the way and for the purposes set out by the initial warrant;
- regular assessments regarding the purposes for which commercially sourced data is used.

151 CTIVD, *Toezichtsrapport nr. 79 over de inzet van virtuele agenten door de AIVD en de MIVD* (2024), https://www.ctivd.nl/documenten/rapporten/2024/09/09/index.

152 CTIVD. *Rapport nr 55 over verwerven van door derden aangeboden bulkdatasets door AIVD en MIVD* (2017), https://www.aivd.nl/documenten/2018/02/13/ctivd-rapport-55-over-het-verwerven-van-door-derden-aangeboden-bulkdatasets-door-aivd-en-mivd.

153 CTIVD, *Toezichtsrapport nr. 79 over de inzet van virtuele agenten door de AIVD en de MIVD* (2024), https://www.ctivd.nl/documenten/rapporten/2024/09/09/index.

154 CTIVD, *Toezichtsrapport nr. 79 over de inzet van virtuele agenten door de AIVD en de MIVD* (2024), https://www.ctivd.nl/documenten/rapporten/2024/09/09/index.

**When it comes to reporting, oversight bodies should**

- report on the practice of data purchases to the maximum extend that they legally can. They may find that new public attention regarding commercially sourced data use by intelligence services merits further ad hoc reporting on this.

**Good practice:**

- In **the Netherlands,** the CTIVD has published a series of public oversight reports focusing on the use of how commercially sourced data by the Dutch intelligence agencies. These reports provide a comprehensive overview of how commercially sourced information is utilized and its relevance to the work of intelligence services. The reports publicly identify and criticize instances of illegal and negligent behaviour and offer recommendations for an improved governance.

Apart from these recommendations and good practices, further regulatory action is certainly necessary to ensure that some data is simply not available on the data market. This goes beyond the scope of this report, however. Plus, there is also a need for a common information security and auditing framework for private sector entities that offer datasets there.

---

# 7. Conclusion

The governance of intelligence agencies' use of commercially sourced data is a multifaceted challenge for our democracies. It raises profound legal and policy questions: Should government agencies have access to such data? How can the political masters of modern intelligence and security services ensure that it is handled and shared responsibly? How must legal frameworks and oversight practice be adjusted to ensure the proportionate and rights-based acquisition, access and use of commercial datasets.

The rapid integration of AI-driven surveillance and use of cross-system big data analysis tools adds further complexity to the governance challenge. Public-private modes of cooperation are becoming even more difficult to disentangle and compound the much-needed effort to rein in disproportionate government access to data held by the private sector.

The empirical results presented in Chapter 4 of this report show that many democracies face substantial deficits in their democratic governance and control of intelligence services' access and use of commercially sourced data. Legal frameworks, oversight mandates as well as the review and audit practices are often not fit for purpose. They are ill-equipped for the growing reliance on a flourishing commercial data ecosystem which also causes many additional risks to national security. Regulatory regimes are marked by fragmentation, ambiguity and accountability gaps. This may further incentivise disproportionate intrusions into the fundamental rights of individuals.

Our review of recent legal adjustments and reform debates in the United Kingdom, the Netherlands, the United States and Germany in Chapter 5 reveals that some lawmakers and policymakers are more prepared than others to address pressing challenges and to entertain new approaches to mitigate new risks.

The good practices and policy recommendations presented in Chapter 6 are hopefully insightful for those who dare to chart a new course for national reforms in their jurisdictions. Of course, countries differ enormously with respect to their legal traditions and their institutional frameworks for intelligence and national security. They also ensure the protection and promotion of the rule of law, democracy and fundamental rights in different ways. There can, therefore, not be a one-size-fits-all solution for addressing the challenge of ad-based surveillance. What the good practice examples demonstrate, however, is that meaningful improvements are possible. Where political will exists, regulatory frameworks and accountability mechanisms can be adjusted to better address and avert the many risks that this paradigm shift in modern intelligence practice entails.

---

# 8. Bibliography

Ayoub, Emile, *Assessing the Intelligence Community's Policy Framework for Commercially Available Information* (24 May 2024), Just Security, https://www.justsecurity.org/96015/commercially-available-information/.

Born, Hans, and Ian Leigh, *Chapter 5: Democratic Accountability of Intelligence Services* (2006), SIPRI Yearbook 2007, https://www.sipri.org/sites/default/files/YB07%20193%2005.pdf.

Brennan Center for Justice, Demand Progress Education Fund, Electronic Privacy Information Center, Surveillance Technology Oversight Project, Advocacy for Principled Action in Government, Center for Democracy and Technology, Due Process Institute et al., *Joint Comment Regarding the Office of Management and Budget's Request for Information on Executive Branch Agency Handling of Commercially Available Information* (16 December 2024), https://epic.org/documents/join-comment-regarding-ombs-request-for-information-on-executive-branch-agency-handling-of

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), *Tätigkeitsbericht 2025: 34. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit* (6 May 2026), https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Taetigkeitsberichte/34.TB/34TB_25.pdf.

Bundesregierung (German Government), *Entwurf eines Gesetzes zur Änderung des BND-Gesetzes, Drucksache 20/8627 (2023),* https://dserver.bundestag.de/btd/20/086/2008627.pdf.

Cameron, Dell, *The FBI Just Admitted It Bought US Location Data* (2023), https://www.wired.com/story/fbi-purchase-location-data-wray-senate/.

Christl, Wolfie, Astrid Perry, Luis Fernando Garcia, Siena Anstis, and Ron Deibert, *Uncovering Webloc: An Analysis of Penlink's Ad-Based Geolocation Surveillance Tech* (9 April 2026), Citizen Lab, https://citizenlab.ca/research/analysis-of-penlinks-ad-based-geolocation-surveillance-tech/.

Cohen, Lena, *Online Behavioral Ads Fuel the Surveillance Industry – Here's How* (6 January 2025), Electronic Frontier Foundation, https://www.eff.org/deeplinks/2025/01/online-behavioral-ads-fuel-surveillance-industry-heres-how.

Computers, Privacy and Data Protection (CPDP) Conference, *Advertisement Intelligence by European Security Agencies* (4 June 2025), https://www.youtube.com/watch?v=EdTLOQGLUVI.

Cox, Joseph, *CBP Tapped into the Online Advertising Ecosystem to Track Peoples' Movements* (3 March 2026), 404 media, https://www.404media.co/cbp-tapped-into-the-online-advertising-ecosystem-to-track-peoples-movements/.

Cyphers, Bennett, *How the Federal Government Buys Our Cell Phone Location Data* (13 June 2022), Electronic Frontier Foundation, https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data.

D66, VVD, and CDA, *2026-2030 Coalition Agreement: Let's Get to Work. Building a Better Netherlands* (30 January 2026), https://www.government.nl/documents/publications/2026/02/23/2026-2030-coalition-agreement-lets-get-to-work---building-a-better-netherlands.

Danish Intelligence Oversight Board tet, *Standards for Danish intelligence review activities* (February 2024), https://tet.dk/wp-content/uploads/2025/04/TET_Standard_2024_UK.pdf.

Dawson, Joanna, *House of Commons Research Briefing on the Investigatory Powers (Amendment) Bill* (21 March 2024), https://researchbriefings.files.parliament.uk/documents/CBP-9960/CBP-9960.pdf.

Deeks, Ashley, *The Double Black Box: National Security, Artificial Intelligence, and the Struggle for Democratic Accountability* (3 February 2025), OUP, https://academic.oup.com/book/59551.

Deutscher Bundestag, *Deutscher Bundestag - Bundestag novelliert die Rechtsgrundlagen der Nachrichtendienste* (16 November 2023), https://www.bundestag.de/dokumente/textarchiv/2023/kw46-de-bnd-976564.

DLA Piper, *Data protection laws in Belgium*, https://www.dlapiperdataprotection.com/index.html?t=law&c=BE.

Dutch Government, Kamerstuck, *Kamerbrief opvolging aanbevelingen CTIVD over inzet virtuele agenten door AIVD en MIVD* (3 November 2025), https://www.rijksoverheid.nl/documenten/kamerstukken/2025/03/11/kamerbrief-toezegging-over-de-opvolging-van-aanbevelingen-in-toezichtrapport-79-over-de-inz

Dutch Government, Kamerstuk, *Regels met betrekking tot de inlichtingen - en veiligheidsdiensten alsmede wijziging van enkele wetten* (12 March 2018), https://zoek.officielebekendmakingen.nl/kst-34588-79.html.

Dutch Government, Staatscourant van het Koninkrijk der Nederlanden, *Regeling van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie* (3 November 2020), https://zoek.officielebekendmakingen.nl/stcrt-2020-56482.html.

Dutch Parliament, Temporary Act on AIVD and MIVD investigations against countries with an offense cyber program, bulk datasets and other specific provisions (2024), https://wetten.overheid.nl/BWBR0049562/2024-07-01.

Dutch Review Committee on the Intelligence and Security Services (CTIVD), *Toezichtsrapport nr 55: Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD* (28 December 2017), https://www.aivd.nl/documenten/2018/02/13/ctivd-rapport-55-over-het-verwerven-van-door-derden-aangeboden-bulkdatasets-door-aivd-en-m

Dutch Review Committee on the Intelligence and Security Services (CTIVD), *Review Report no 74: Automated OSINT: tools and sources for open source investigation* (22 December 2021), https://english.ctivd.nl/documents/2022/09/19/index.

Dutch Review Committee on the Intelligence and Security Services (CTIVD), *Toezichtsrapport nr 79 over de inzet van virtuele agenten door de AIVD en de MIVD* (25 July 2024), https://www.ctivd.nl/documenten/2024/09/09/index.

Dutch Review Committee on the Intelligence and Security Services (CTIVD), *Brief CTIVD vz TK inzake publiek-private samenwerking* (17 February 2025), https://www.ctivd.nl/site/binaries/site-content/collections/documents/2025/02/17/index/20250217_O_Brief+vz+TK+inzake+Publiek-Private-Samenwerking.pdf

Efinger, Svenja, and Thorsten Wetzling, *Wanted: A legal authority for data purchases by German security and intelligence agencies* (20 January 2026), about:intel, https://aboutintel.eu/commercial-data-adint-germany-intelligence-reform/.

EOS Committee, *Annual Report 2022* (29 March 2023), https://eos-utvalget.no/wp-content/uploads/2023/06/EOS-Committee-annual-report-2022.pdf.

EOS Committee, *Annual Report 2024* (26 March 2025), https://eos-utvalget.no/wp-content/uploads/2025/06/EOS-annual-report-2024.pdf.

Executive Office of the President, *Executive Order 14117: Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (28 February 2024), https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-relat

Frenkel, Sheera, and Aaron Krolik, *How ICE Already Knows Who Minneapolis Protesters Are*. Technology (30 January 2026), The New York Times, https://www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html.

Gastineau, Pierre, *Loi de programmation militaire: le cahier de doléances de la DGSE* (4 July 2022), Intelligence Online, https://www.intelligenceonline.fr/europe-russie/2022/07/04/loi-de-programmation-militaire--le-cahier-de-doleances-de-la-dgse,109796352-eve.

Geiger, Gabriel, Crofton Black, Riccardo Coluccini, Bashar Deeb, Elena de Bre, Sabrina Slipchenko, Sarasvati Thuppadolla et al., *How First Wap Tracks Phones Around the World* (14 October 2025), Lighthouse Reports, https://www.lighthousereports.com/methodology/surveillance-secrets-explainer/.

Internet Society, *Investigatory Powers (Amendment) Act 2024: Consultation Response to the Home Office* (6 January 2025), https://www.internetsociety.org/resources/doc/2025/investigatory-powers-amendment-act-2024-consultation-response-to-the-home-office/.

Investigatory Powers Commissioner's Office (IPCO), *Annual Report of the Investigatory Powers Commissioner 2019* (15 December 2020), https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf.

Investigatory Powers Commissioner's Office (IPCO), *Annual Report of the Investigatory Powers Commissioner 2024* (16 December 2025), https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2024.pdf.

Lorenzo Perez, Silvia, *What the PCLOB Firings Mean for the EU-US Data Privacy Framework* (14 February 2025), Center for Democracy & Technology, https://cdt.org/insights/what-the-pclob-firings-mean-for-the-eu-us-data-privacy-framework/.

MacDonald-Evoy, Jerod, *Tucson PD Used Border Security Money for Controversial Surveillance Software* (29 October 2025), AZ Mirror, https://azmirror.com/2025/10/29/tpd-used-border-security-money-for-controversial-surveillance-software/.

Mansoor, Sanya, *Why Is the FBI Buying People's Location Data and How Is It Using the Information?* (19 March 2026), https://www.theguardian.com/technology/2026/mar/19/fbi-buying-location-data-use.

Meineck, Sebastian, and Ingo Dachwitz, *Data Broker Files: How data brokers sell our location data and jeopardise national security* (16 July 2024), https://netzpolitik.org/2024/data-broker-files-how-data-brokers-sell-our-location-data-and-jeopardise-national-security/.

Metz, Cade, and Julian E. Barnes, *OpenAI Amends A.I. Deal With the Pentagon* (2 March 2026), New York Times, https://www.nytimes.com/2026/03/02/technology/openai-pentagon-deal-amended-surveillance.html.

National Resource Governance Institute, *Legal Framework: Navigating the Web of Laws and Contracts Governing Extractive Industries* (March 2015), https://resourcegovernance.org/sites/default/files/nrgi_Legal-Framework.pdf.

National Security and Intelligence Review Agency, *Review of Canadian Security Intelligence Service Dataset Regime* (27 March 2024), https://nsira-ossnr.gc.ca/en/reviews/find-a-review/21-15/report/.

National Security and Intelligence Review Agency, *Review of CSIS Dataset Regime* (2024), https://publications.gc.ca/collections/collection_2024/ossnr-nsira/PS108-6-2024-eng.pdf.

New Zealand Inspector-General of Intelligence and Security, *IGIS concerned at NZSIS use of class warrants* (27 March 2024), https://igis.govt.nz/publications/media-releases/announcements/igis-concerned-at-nzsis-use-of-class-warrants.

Office of the Director of National Intelligence (ODNI), *Intelligence Community Policy Framework for Commercially Available Information* (May 2024), https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf.

Panyi, Szabolcs, *Orbán's Spying Kit Revealed: Israeli Surveillance Tool Combined with Hungarian Technology* (9 April 2026), Vsquare, https://vsquare.org/orban-spying-toolkit-cobwebs-webloc-hungary-spyware-citizen-lab/.

Privacy and Civil Liberties Oversight Board (PCLOB), *Report on the National Counterterrorism Center* (10 December 2024), https://documents.pclob.gov/prod/Documents/OversightReport/4ce093a4-d28d-4996-a35b-c11d18e19018/PCLOB%20FY2024%20NCTC%20REPORT%20-%20Completed%20508%20-%20Dec%2017

Privacy and Civil Liberties Oversight Board (PCLOB), Staff Report, *Use of Open Source Information by the Federal Bureau of Investigation* (20 November 2026),

https://documents.pclob.gov/prod/DynamicImages/Generic/fd7d5577-e5c9-4247-ade7-b71e5937e41e/%28U%29%20Use%20of%20Open%20Source%20In

Privacy International, and Rights & Security International, *Dangerous Data: Police Abuse of Access to Personal Data in the United States and its Global Implications* (April 2026), https://privacyinternational.org/sites/default/files/2026-04/Dangerous%20Data%20-%20RSI%20and%20PI%20-%20April%202026.pdf.

Privacy International, *PI's Response to the UK Government's Investigatory Powers (Amendment) Bill* (22 February 2024), http://privacyinternational.org/advocacy/5258/pis-response-uk-governments-investigatory-powers-amendment-bill.

Privacy International, *Privacy International's Response to the Consultation on the Investigatory Powers (Amendment) Act 2024: Codes of Practice and Notices Regulations*, https://privacyinternational.org/sites/default/files/2025-01/PI%20Consultation%20Response%20-%20IPAA%20Codes%20%28submitted%29.pdf.

Proschofsky, Andreas, *Innenministerium nutzt Überwachungssoftware von zwielichtiger Firma, will nicht darüber reden* (20 February 2026), Der Standard, https://www.derstandard.at/story/3000000309258/innenministerium-nutzt-ueberwachungssoftware-von-zwielichtiger-firma-will-nicht-darueber-re

Ruckerbauer, Corbinian, and Thorsten Wetzling, *Informationsbeschaffung mit der Kreditkarte: Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen* (28 May 2024), interface. https://www.interface-eu.org/publications/nachrichtendienstliche-datenkaeufe.

Schrader, Hannes, *Anschlag auf Berliner Stromnetz: Kabelbrücke war monatelang nahezu ungeschützt zugänglich* (5 February 2026), Der Spiegel, https://www.spiegel.de/panorama/justiz/stromausfall-in-berlin-kabelbruecke-monatelang-nahezu-ungeschuetzt-und-zugaenglich-a-02826

Shenkman, Carey, Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers (*December 2021), Center for Democracy & Technology, https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

Swiss Independent Oversight Authority for Intelligence Activities, *Annual Report 2024* (19 May 2025), https://2024.ab-nd-taetigkeitsbericht.ch/en/.

Tau, Byron, *Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State*, 2024, Crown.

Technological Advisory Panel (TAP) of the UK's Investigatory Powers Commissioners

Office (IPCO), *AI Proportionality Assessment Aid* (April 2025), https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/AI-Assessment-Framework.pdf.

U.S. Department of Homeland Security, *Privacy Act of 1974: Implementation of Exemptions; System of Records; Office of Intelligence and Analysis Enterprise Records System* (30 September 2008), https://www.govinfo.gov/content/pkg/FR-2008-09-30/html/E8-22603.htm

U.S. Department of Homeland Security Privacy Office, *Privacy Threshold Analysis: AdID Efficacy Pilot*, https://www.documentcloud.org/documents/27714350-adid-efficacy-pilot-pta/.

U.S. Department of Justice, *Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries* (11 April 2025), https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive.

U.S. Department of Justice, *Notice of Proposed Rulemaking: Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons* (October 2024), https://www.justice.gov/d9/2024-10/nsd_104_-_data_security_-_1124-aa01_-_notice_of_proposed_rulemaking_0.pdf.

U.S. Department of the Treasury, *System of Records Notices*, https://home.treasury.gov/footer/privacy-act/system-of-records-notices-sorns.

U.S. Government Accountability Office (GAO), *DOD Intelligence: Action Needed to Strengthen Program Oversight and Manage Risks* (February 2024), https://www.gao.gov/assets/gao-24-106190.pdf.

U.S. Government Accountability Office (GAO), *Information Environment: DOD Needs to Address Security Risks of Publicly Accessible Information* (October 2025), https://www.gao.gov/assets/890/882289.pdf.

U.S. Senate Committee on Armed Services' Subcommittee of Emerging Threats and Capabilities, *To Receive Testimony on Threats and Challenges Posed to Department of Defense Personnel and Operations From Adversarial Access To Publicly Available Data Coupled with Advances Data Analysis Tools Now Widely Available on the Commercial Market* (7 October 2025), https://www.armed-services.senate.gov/hearings/to-receive-testimony-on-threats-and-challenges-posed-to-department-of-defense-personnel-and-

UK Department for Science, Innovation & Technology, *Call for evidence outcome: Data brokers and national security* (4 December 2025), https://www.gov.uk/government/

calls-for-evidence/data-brokers-and-national-security/data-brokers-and-national-security.

UK Home Office, *Intelligence Services' Use of Third Party Bulk Personal Datasets: Code of Practice* (June 2025), https://assets.publishing.service.gov.uk/media/6841a87241cb2525c1211cf5/Intelligence_Services__use_of_Third_Party_Bulk_Personal_Datasets_Code_of_Practice_-_June

UK Home Office, *Investigatory Powers (Amendment) Bill: Bulk Personal Datasets and Third Party Bulk Personal Datasets* (26 April 2024), https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill-bulk-personal-datasets-and-third-party-bulk-personal-data

UK Parliament, *Investigatory Powers (Amendment) Bill: Explanatory Notes* (2024), https://publications.parliament.uk/pa/bills/cbill/58-04/0157/en/230157en.pdf.

Untersinger, Martin, *How surveillance companies track smartphone users through advertising data*, (22 January 2026), Le Monde, https://www.lemonde.fr/en/pixels/article/2026/01/22/how-surveillance-companies-track-smartphone-users-through-advertising-data_6749674_13.htm

Wetzling, Thorsten, and Charlotte Dietrich, *Disproportionate Use of Commercially and Publicly Available Data: Europe's next Intelligence Reform?* (17 November 2022), interface, https://www.interface-eu.org/publications/disproportionate-use-commercially-and-publicly-available-data-europes-next-frontier.

Wetzling, Thorsten, and Charlotte Dietrich, *Report on the need for a Guidance note on Article 11 of the modernised Convention 108* (11 June 2021), Council of Europe, https://rm.coe.int/t-pd-2021-6-draft-guidance-note-on-exceptions-under-article-11-of-the-/1680a2d512.

Wissenschaftliche Dienste des Deutschen Bundestags, *Rechtliche Voraussetzungen und Grenzen des behördlichen Ankaufs von personenbezogenen Daten aus Werbedatenbanken* (27 November 2025), https://www.bundestag.de/resource/blob/1134752/WD-3-065-25.pdf.

# 9. Annex

## 9.1. Questionnaire for Oversight Practitioners

**Q1.** Do you know of another dimension that pertains to the protection of fundamental rights and freedoms that we should include in the analysis scheme?

**Q2.** Are specific types of data purchases or forms of accessing commercially sourced data subject to ex-ante authorization in your country?

Yes ___ No___

If yes, which conditions have to be met?

---

**Q3.** Is there an explicit prohibition, restriction or limitation in your country's regulatory framework regarding types of data and methods of data collection for IC arrangements/ contracts with PSEs?

Yes ___ No___

If yes, please point us to the relevant provisions in the legal framework.

---

**Q4.** Is there an explicit prohibition, restriction or limitation in your country's regulatory framework regarding the provenance of PSEs from whom data must not be purchased?

Yes ___ No___

If yes, please point us to the relevant provisions in the legal framework.

If no, can you point us to other sources that contain such restrictions or limitations?

---

**Q5.** Are IC actors obligated to assess PSEs against specific standards, such as transparency, before entering contracts/arrangements/transactions?

Yes___ No___

If yes, please point us to such standards in your national legal framework.

---

**Q6.** Can your institution access executive decrees or internal administrative policies on the use of commercially sourced data and/or data purchasing from PSEs?

Yes___ In parts___ No___

---

**Q7.** Does your institution have a formal mandate to oversee IC activities related to the pre-access phase?

Yes___ No___

---

**Q8.** Does your institution need to be:

informed: Yes___ No___

consulted: Yes___ No___

co-deciding: Yes___ No___

other:

when a contract between an IC actor and a PSE involving access and use to commercially sourced data is to be concluded?

If yes, is your institution also

informed: Yes___ No___

consulted: Yes___ No___

co-deciding: Yes___ No___

other:

when a contract is to be renewed?

---

**Q9.** Does your institution have the binding power to delay or stop the conclusion of a contract?

Yes___ No___

---

**Q10.** Have you conducted investigations into internal policies and/or statutory provisions on the acquisition of commercially sourced data?

Yes___ No___

---

**Q11.** Is there a dimension or risk in the access phase that pertains to the protection of basic rights and fundamental freedoms that you find missing?

---

**Q12.** Do you think that data minimisation requirements normally required for sovereign data in your country can be circumvented when commercially sourced data is stored and

accessed by IC actors on PSE servers?

Yes___ No___

---

**Q13.** Do you find that there should be different regulations and oversight requirements in the national legal frameworks for "sovereign data acquisition" and "mediated data access"?

Yes___ No___

If yes, how should the requirements for regulation and oversight be different in your view?

---

**Q14.** Are IC actors in your country obliged to maintain an inventory of all databases?

Yes___ No___

If so, does this include databases run on the systems or with the support of PSE?

---

**Q15.** Are there any specific rules for standardised data minimisation procedures when acquiring data from PSEs?

Yes___ No___

---

**Q16.** Does your oversight institution have a complete overview of which data is transferred to PSEs for data processing purposes?

Yes___ No___

---

**Q17.** Is your oversight institution able to trace data minimisation efforts for both the IC's sovereign or mediated use of commercially sourced data?

Yes___ No___

---

**Q18.** Is your institution able to identify which categories of data are contained in big datasets?

Yes___ No___

If yes, do you know how many persons are affected?

Yes___ No___

If yes, do you know whether the individuals affected are nationals or non-nationals?

Yes___ No___

---

**Q19.** To mitigate the risks of erroneous decision-making due to the use of manipulated, or unintentionally incorrect or biased data, is your oversight institution able to evaluate the IC's efforts to test the integrity of the data?

Yes___ No___

---

**Q20.** Is there a dimension or risk in the data processing phase that pertains to the protection of basic rights and fundamental freedoms that you find missing?

---

**Q21.** Are the intelligence services obliged to reassess a dataset after significant changes have been made to it or when substantial new information has been derived from it?

Yes___ No___

---

**Q22.** What exactly should IC actors acquiring commercially sourced data be required to document in written form and what exactly should they report to whom on their processing of that information?

---

**Q23.** Can your institution access log recordings on the processing of commercially sourced datasets?

Yes___ No___

---

**Q24.** Does your oversight institution encounter difficulties when assessing the tools PSE use to process commercially sourced information?

Yes___ No___

---

**Q25.** Is there a dimension or risk in the data sharing phase that pertain to the protection of

basic rights and fundamental freedoms that you find missing?

---

**Q26.** Does the regulatory framework in your country provide specific regulations for the sharing of commercially sourced data with

other government agencies: Yes___ No___

international partner agencies: Yes___ No___

PSE actors? Yes___ No___

If there is specific regulation in place, please point us to relevant provisions?

If there is no specific regulation in place, do you find that existing provisions in your national legal framework on intelligence sharing between IC actors and other actors adequately address the specific risks that arise when IC actors share commercially sourced data?

Yes___ No___

If yes, please point us to these provisions.

---

**Q27.** Does the oversight remit of your oversight institution cover inspections and audits into the sharing of commercially sourced data with partner institutions within government and with foreign partners?

Yes___ No___

If yes, has your institution performed an audit into commercially sourced data transfers?

Yes___ No___

---

**Q28.** Do you think that your oversight institution has a sufficiently comprehensive overview of transfers of commercially sourced data with other national or international partners?

Yes___ No___

If not, where do you think are the blind spots and how could they be reduced or even filled?

---

**Q29.** Is there a dimension or risk in the deletion phase that pertain to the protection of basic rights and fundamental freedoms that you find missing?

---

**Q30.** Are there specific data retention and deletion provisions in your national legal framework on commercially sourced information?

Yes___ No___

If yes, please point us to relevant provisions.

---

**Q31.** Are there specific record-keeping provisions in your national legal framework regarding the deletion of commercially sourced data?

Yes___ No___

---

**Q32.** If yes, do these record-keeping requirements regarding data deletion apply also to PSEs when IC actors have outsourced data processing to them?

Yes___ No___

---

**Q33.** If you become aware of an illegal or disproportionate data deletion practice, can your institution initiate an investigation into such practices?

Yes___ No___

---

**Q34.** Does your institution possess a binding power to order the deletion of commercially sourced data that - according to the law - should no longer be retained and/or deleted?

Yes___ No___

If yes, does this power extend to a PSE in case of mediated data use

Yes___ No___

---

**Q35.** Is there a dimension or risk in the deletion phase that pertains to the protection of basic rights and fundamental freedoms that you find missing?

*Your answer…*

---

**Q36.** Can your oversight institution publicly report on the scope of data purchases within your national IC?

Yes___ No___

If no, what are the reasons for its omission?

---

**Q37.** Have you done public reporting on the scope of data purchases within your national IC?

Yes___ No___

If yes, were you able to include an overview over data purchasing trends over a longer period of time?

Yes___ No___

If yes, have trade secrets influenced your ability to report on specific practices?

Yes___ No___

---

**Q38.** Do you know another good practice on the regulation of the IC's use of commercially sourced data?

If yes, please send us the relevant information and, ideally, a brief justification as to why you think this amounts to a good practice.

---

**Q39.** Do you know another good practice regarding the mandate or work of independent and effective oversight institutions on the matter of the IC's use of commercially sourced data?

If yes, kindly point us to relevant information and, ideally, a brief justification as to why you think this amounts to a good practice.

# Authors

Corbinian Ruckerbauer
Senior Policy Researcher Digital Rights, Surveillance and Democracy
cruckerbauer@interface-eu.org
+49 30 81 45 03 78 80

Dr. Thorsten Wetzling
Lead Digital Rights, Surveillance and Democracy
twetzling@interface-eu.org
+49 (0)30 81 45 03 78 80

# Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 ( 0 ) 30 81 45 03 78 80
F +49 ( 0 ) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
c/o Publix
Hermannstraße 90
D-12051 Berlin



Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com