SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE RULE OF LAW ACROSS DEMOCRATIC STATES

The University of Texas at Austin
Strauss CENTER
for International Security and Law

NATIONAL SECURITY SURVEILLANCE IN SWEDEN

Iain Cameron

ABOUT THE AUTHOR

Iain Cameron is Professor in Public International Law at Uppsala University. His research interests lie in human rights/civil liberties, international criminal law and police/security issues. Since 2005, he has been one of the two Swedish members of the Commission on Democracy through Law (Venice Commission).

ACKNOWLEDGEMENTS

This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

NOVEMBER 2023

I. INTRODUCTION

The Swedish legal frameworks for approving and overseeing domestic and foreign electronic intelligence collection appear to be relatively strong when compared with those in other democratic states. Domestic surveillance for such purposes as counterterrorism and counterintelligence is regulated by criminal procedure; collection of signals for foreign-intelligence purposes is governed by a separate statutory regime, the Signals Intelligence Act.

Separate oversight bodies exist for domestic security surveillance and foreign intelligence collection. Annual reports provide varying degrees of statistical detail, depending on the category of surveillance. Swedish law also provides a "redress" mechanism permitting both Swedes and non-Swedes to file complaints about alleged illegal surveillance.

II. INSTITUTIONS

Operational Entities

There are two Swedish agencies with primary responsibility for conducting electronic surveillance for national security purposes: (1) the Security Service (*Säkerhetspolisen*) and (2) the signals intelligence agency, the Defence Radio Establishment (*Försvarets radio anstalt*, or FRA).

The Security Service has primacy in investigating threats to national security in Sweden. Its main responsibilities are counterintelligence, counterterrorism, VIP protection, countersubversion, protective security (information security/vetting) and counterproliferation. The origins of the Security Service go back to WWII. It was originally an autonomous sub-unit of the national police but the two agencies were formally separated in 2015. The Security Service has police powers (of arrest, to use special investigative methods, etc.) but now largely consists of civilian employees, reflecting its more long-term analytical role. Responsibility for investigating smuggling offences, including violations of export controls or sanctions, is shared with the Customs Service.

> ***There are two Swedish agencies with primary responsibility for conducting electronic surveillance for national security purposes: (1) the Security Service (Säkerhetspolisen) and (2) the signals intelligence agency, the Defence Radio Establishment (Försvarets radio anstalt, or FRA).***

Since 2015, the Swedish Police is a national organisation, administratively divided into seven regions and subdivided into smaller areas. There is a relatively clear demarcation of responsibility between the police and the security service but in some circumstances jurisdictions overlap. For example, organised crime is a matter only for the Police whereas investigation of terrorism is a shared responsibility. The Customs Services and the Police receive technical expertise and assistance from the Security Service for electronic surveillance in domestic investigations.

The FRA is the primary agency for gathering electronic foreign intelligence, as well as responding to cyber threats directed against Swedish interests. The origins of FRA go back to the beginning of WWII. It originally operated only as a supplier of intelligence to the military intelligence and security service, (Militära underrättelse och säkerhetstjänsten, MUST), and the Armed Forces. By the 1980's, however, FRA was developing its own analytical capabilities.

Authorizing and Oversight Entities

The authorizing and oversight bodies track the parallel systems for domestic and foreign intelligence. In part, this is for historical reasons; however, it also reflects the need in domestic contexts for a greater focus on the constitutional rights of citizens and principles of criminal law and criminal procedure. This arrangement could also reflect simple inertia and "cultural" differences between the defence and justice ministries.

Two distinct entities conduct oversight of the FRA's foreign intelligence mission. The independent Foreign Intelligence Court (Försvarsunderrättelsedomstolen or FUD), grants warrants. The Defence Intelligence Inspection (Statens inspektion för försvarsunderrättelseverksamheten, SIUN), performs follow-up oversight of how the warrant is implemented.

This dual oversight structure dates to 2008. Originally, the FRA only monitored radio and telemetry signals and was overseen only by SIUN, which also oversees MUST. With the growth of the internet, the government decided in 2008 to propose legislation giving FRA competence to monitor cable traffic. This caused a political outcry, and as part of an all-party compromise in the parliament, an independent authorising body, FUD, was established.

For domestic threats to national security, including counterintelligence, the main basis for granting warrants to collect electronic surveillance is the criminal law (i.e., national security offences), and criminal procedure law, albeit with some modifications. This means that the Security Service needs the

permission of a specialist prosecutor, who will usually in turn need a warrant from a district court.

An independent body, the Commission on Security and Integrity Protection (Säkerhets- och integritetsskyddsnämnden or SIN), oversees the use of surveillance in investigations conducted under the criminal law. The forerunner to SIN was a specialist data protection body, the Register Board, established in the 1990's to monitor police and Security Service data files. The Register Board was established mainly because of human rights/due process concerns related to the reliability of these data files, especially in security vetting.

SIN was created in 2005 as part of a package deal granting the police and Security Service increased surveillance powers. There was a realisation that the prosecutorial and judicial control only checked if there was reasonable cause to *initiate* surveillance, and there was no post hoc monitoring with focus on "lessons learnt." SIN was thus given a follow-up oversight function over use of electronic surveillance for domestic investigations.

III. OPERATIONAL CAPABILITIES AND PRIORITIES

Sweden is a relatively small country in terms of population, with only 10.5 million people. Its armed forces are small. Relatively speaking, the Swedish navy and air force receive most resources. The manpower of the army is very limited. Sweden has put its faith, until recently, in its non-aligned political stance, even if cooperation with NATO (within the framework of Partnership for Peace) has been considerable since 1995. Sweden modified its non-aligned stance in 1995 when it joined the EU. As a result of the Russian invasion of Ukraine in February 2022, Sweden applied for NATO membership. Sweden is thus now committed to increasing defence spending to 2% of GNP, as well as increased intelligence cooperation.

Bearing in mind the size of the armed forces, the Swedish intelligence community is large, relatively speaking. FRA has around 900 employees.[1] The Security Service has around 1,400 employees.[2] MUST is formally part of the Swedish Armed Forces, even though many of the people employed in MUST have civilian status. The number of employees in MUST is secret.

The geographical location of Sweden has increased its importance for signals intelligence gathering, particularly against the Russian Federation. Much Russian cable traffic is channelled through Swedish territory and territorial waters, and thus susceptible to interception by FRA. Swedish listening stations on islands and aboard aircraft and ships have capability to intercept significant portions of Russian radio traffic in the Baltic region. The proximity of Sweden's northern territorial boundaries to the Arctic Circle means that communications using certain geo-stationary satellites can also be monitored.

Publicly available information on FRA's technical and operational capacities is very limited. Anecdotal evidence suggests that at least half of the FRA's capacity is devoted to purely military targets, which can be assumed to be largely Russian. FRA has a long and continuous history of code-breaking and a relatively high level of technical competence. Swedish know-how generally in telecommunications is sophisticated, with the company Ericsson still being world-leading in some respects.

Unlike the Swedish army, FRA did not atrophy during the (temporary) end to the Cold War in the 1990s—it maintained its expertise. Despite Sweden's formal political policy of non-alignment, FRA cooperated with (and received technical assistance and help from) the British GCHQ during the Cold War, and it continues to cooperate closely with GCHQ. FRA's size means that it can only be a junior partner to GCHQ, the German BND, and, obviously, the U.S. NSA. However, the anecdotal information I have received is that FRA occasionally makes appreciated contributions to the work of these foreign agencies.

The geographical location of Sweden has increased its importance for signals intelligence gathering, particularly against signals intelligence from the Russian Federation.

The Security Service publishes a short annual report, which illustrates how its activities relate to contemporary geopolitical and security concerns. In recent years, terrorism has been a high priority. Significant numbers of Swedish citizens and residents participated as "foreign fighters" in conflicts in Iraq and Syria, many in extremist jihadist groupings such as the Islamic State. The Swedish high-tech industry and universities are the object of aggressive industrial espionage from China, Iran, and Russia. The Swedish economy is heavily export-based, necessitating monitoring of export controls and sanctions.

There is a publicly available Swedish national security strategy. The latest version of this is from 2017. It is written at a relatively high level of abstraction.

IV. PROCESS FOR CONDUCTING SURVEILLANCE

Swedish law distinguishes between overseas and domestic collection of electronic surveillance. There is no third legal category equivalent to the U.S. "section 702": domestic collection directed against targets physically situated abroad.

Under Swedish law, defence intelligence activities (carried out either by MUST or FRA) may not be used against purely domestic threats to national security.[3] Moreover, collection of signals intelligence is only permitted for communications crossing the Swedish border.[4] If *both* the sender and the receiver are physically located in Swedish territory, any communications collected (by interception of either radio or cable) must be destroyed.[5]

By contrast, the type of situation covered by U.S. "section 702" surveillance, where one participant in the communication (or accessing of website, etc.) is physically located abroad, can be legally treated as *either* domestic or foreign intelligence. When the law was changed to allow FRA to intercept cable traffic, the bill recognised[6] that there is an overlap between signals intelligence collection, which can involve "strong" identifiers linked to a specific person (see below), and domestic interception of communications, which is always directed against a specific person. This overlap is handled by a legal provision and an administrative practice giving primacy to domestic surveillance procedures. This rule holds that once there is sufficient evidence to justify the initiation of a prosecutorial-led preliminary investigation against a specified person for a specific offence,[7] signals intelligence collection directed against that same target must cease.[8] SIN and SIUN pay special attention to monitoring this issue.

Domestic collection

Sweden's Code of Criminal Procedure provides that: "Covert interception of electronic communications … may only be conducted if someone is reasonably suspected of an offence."[9] The baseline rule thus requires reasonable suspicion of a specified, concrete, offence and (usually) a suspect. However, a 2012 amendment created an exception allowing interception of metadata in order to determine who may be reasonably suspected of a given, specific offence, where this is of particular importance to the investigation.[10] Lawmakers are considering further exceptions; cumulatively, these exceptions make the baseline rule less clear (and thus also further muddle the point when "foreign" surveillance must cease). A legal person (i.e., a corporation) cannot commit an offence in Sweden, and so cannot be subject to an interception order.

The use of "coercive powers"[11] such as wiretaps and physical searches is generally speaking only permissible to investigate an offence which has already been committed, is in the process of being committed, or in specific cases set out in law, where attempt, preparation, or conspiracy to commit an offence is punishable. However, proactive surveillance is now allowed under the Act (2007:979) on measures to prevent particularly serious crimes, when there is reason to believe that a person will perform criminal acts in the future, including certain listed offences (such as sabotage, arson, terrorist offences, and murder). The 2007 Act is mainly aimed at national security offences.[12]

Generally, interception orders may only be issued for offences punishable by a minimum of two or more years imprisonment, or where it is likely that the sentence will be at least two years imprisonment. In Sweden, only serious offences are punishable by a minimum of 2 years imprisonment. Having said this, by virtue of the Terrorist Crimes Act, the commission of a list of ordinary offences with a terrorist intent carries a minimum penalty of 4 years imprisonment.[13] Thus, if terrorist intent is suspected, a long list of offences can form the basis of an interception order.

The 2007 Act moves the threshold for using interception of communications a little further forward in time for certain specified security-related offences. However, it is unclear how often the Act needs to be invoked. For most serious security-related offences, attempt, preparation, and conspiracy will also be punishable for more than the requisite two years, meaning that interception is likely to be possible even at an early stage.

As regards who can be subject to an interception order (e.g., suspects, their intermediaries, their communication partners, specific devices), CJP 27:20 makes it possible to collect historical metadata on a telephone number/communication address other than that held or used by the suspect if there are "particular reasons" to suspect that s/he will contact that number. CJP 27:20 also allows interception of the content of communications and metadata as well as bugging, subject to similar (though more demanding) conditions.

Since 2020, for a trial period of 5 years, it has been possible to apply for court permission to interfere with computers/smartphones, such as by planting trojans or otherwise obtaining covert access to the content of the device, including its communications in real-time.[14] In recent years, criminals, especially those involved in drug crime, have used dedicated encrypted mobile phones (e.g., Encrochat). Swedish law does not provide for the possibility to gain backdoor access to these platforms generally, as opposed to hacking a specific criminal's endpoint device. However, rules on mutual assistance in law enforcement enabled Sweden to receive such information from law enforcement in other countries (France, Netherlands, the USA, etc.) where this was legal.[15]

As noted in section II, it is a district court which authorizes electronic surveillance, on the application of the prosecutor, and for a maximum (renewable) period of one month.[16] In practice, counter-intelligence warrants are issued by a special chamber of the Stockholm district court. Judges issuing electronic surveillance warrants are security-vetted.

When the Security Service wants access to historical metadata, the process is simpler. For serious offences, the prosecutor can authorize the Security Service to access telecommunications companies' metadata.[17] SIN oversees this access, as described below.

The procedures and safeguards set out in the Code of Criminal Procedure apply to all people present in the territory of Sweden. However, for non-Swedish citizens present in Sweden who are suspected of involvement in terrorism, there is a special rule removing the need for reasonable suspicion that the person in question has committed, or is committing, a specified offence.[18] This however, applies only to a relatively small number of people per year, usually asylum seekers who, for some reason (usually the non-refoulement principle) cannot be deported.

Since 2020, for a trial period of 5 years, it has been possible to apply for court permission to interfere with computers/smartphones, such as by planting trojans or otherwise obtaining covert access to the content of the device, including its communications in real-time.

The SIN conducts post hoc oversight of electronic surveillance conducted under the criminal law. SIN's mandate is (1) to ensure that surveillance activities by the police and the Security Service are conducted in accordance with laws and other regulations and (2) that the police and the Security Service registration and retention of personal data is "conducted in accordance with laws and other regulations."[19]

The SIN is a ten-member board with a mix of judicial and political appointees. The Chair and Vice Chair of SIN must be current or former tenured judges, or people with equivalent legal experience.[20] Appointments to these positions are prepared by the Judicial Appointments Board (which proposes all tenured judicial appointments). The other members are chosen by parties in the Riksdag, each of which typically proposes a member of the Commission. All members are appointed

by the government for a (renewable) fixed period of no more than four years.

The SIN's decisions are taken by majority vote. A quorum requires the Chair and half of the other members to be present. SIN as a monitoring/complaints body meets around once a month. SIN is assisted by a legally qualified director (appointed by the government) and four to five legally qualified desk officers, as well as administrative staff. SIN has no legal power itself to order correction or deletion of data or order the payment of damages if it determines that laws or regulations have not been followed. However, it is obliged to report possible breaches of the criminal law to the prosecutor, and breaches of administrative law to other administrative authorities with wider powers.

Foreign Intelligence

Under section 1 (2) of the Signals Intelligence Act, signals intelligence may only be used for the following purposes:

1. external military threats to the country;
2. conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations;
3. strategic circumstances concerning international terrorism or other serious cross-border crime that may threaten essential national interests;
4. the development and proliferation of weapons of mass destruction, military equipment, and other similar specified products;
5. serious external threats to society's infrastructure;
6. foreign conflicts with consequences for international security;
7. foreign intelligence operations against Swedish interests; and
8. the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy."[21]

In 2021, one further purpose was added:

"9. such phenomena as are referred to in 1-8, but which are not directed at Sweden or concern Swedish interests, if it is necessary for cooperation in intelligence matters with other countries and international organizations in which the signal intelligence authority participates."[22]

Under sections 1(1) and 4(1) of the Signals Intelligence Act, only certain bodies may "task" FRA to collect intelligence, namely the Government, the Government Offices,[23] the Armed Forces, the Security Service, and the National Operative Department of the Police (which deals with serious organised crime). A tasking directive shall include information about (i) the issuing authority, (ii) the part of the Government's annual intelligence needs assessment it concerns, (iii) the phenomenon or situation intended to be covered, and (iv) the need for intelligence on that phenomenon or situation[24] (section 2a).

As regards collection of cable borne electronic signals, telecommunications companies are required by law to route all international communications through certain connecting points.[25] FRA has then the possibility to "mirror" (copy) the parts of the traffic it wishes to collect.

Automated selectors are used to filter the signals bearers and to analyse the data collected. Under section 3 of the Signals Intelligence Act, selectors must be formulated in such a way that the interference with personal integrity is limited as far as possible. Moreover, selectors directly relating to a specific natural person may only be used if this is of "exceptional importance"[26] for the intelligence activities. This provision was intended to reassure the public that signals intelligence searches would not routinely be used to circumvent the tougher requirements set out in domestic law for the use of electronic surveillance to investigate identified individuals for national security crime (espionage etc.).

For any collection of signals intelligence, including for technical purposes ("development activities"),[27] the FRA must apply for a permit to FUD, the independent Foreign Intelligence Court. There is an exception in cases of urgency.[28] An application must contain the request that the FRA has received, with information on the underlying directive and the need for the specific intelligence sought.

The application must also specify the communications bearers to which the FRA requires access,[29] along with the selectors or (at least) *categories* of selectors that will be used. If the application notes the categories of selectors sought, FUD must determine whether the categories alone will suffice or the FRA must instead provide the specific selectors it plans to employ.

Finally, the application must state the duration for which the permit is requested.[30]

The FUD applies the principles of necessity (least intrusive means) and proportionality (balancing the degree of interference with the value of the material which can be obtained) in granting a warrant, and may impose conditions on the warrant.[31] A warrant is issued for a maximum of six months.[32] No case law has been made public, so it is difficult to know how FUD interprets these principles in practice.

The FUD consists of a president, who must be a tenured judge, one or two vice-presidents, who must have a legal background, and two to six other members, who usually have a background as (former) members of parliament for different political parties.[33] The body has thus a "hybrid" composition. All appointments are made by the Government for four-year terms; the president, however, must first be proposed by the independent Judicial Appointments Board. The court meets behind closed doors. To make the procedure somewhat more "adversarial," an independent "privacy protection representative" (*integritetsskyddsombud*) is present, as well as a representative from FRA.

Like FUD, SIUN, the oversight body for foreign intelligence, has a hybrid composition, and is appointed in the same way, with a tenured judge, or former judge, as president, appointed after a proposal by the independent Judicial Appointments Board. There are, however, certain differences in both mandate and composition, compared to the equivalent oversight body for domestic investigations, SIN. SIUN is a smaller body, with only three to four members appointed from political parties (usually former MPs), reflecting the greater sensitivity of the intelligence material. Political representation was felt to be desirable because the intelligence FRA is often tasked to collect is often closely connected to Swedish foreign policy.

SIUN also has a broader oversight mandate. In addition to ensuring that MUST and FRA follow the laws, it has specific obligations to monitor how FRA and MUST handle personal data, including destruction requirements, and how they conduct recruitment and training. Specific Acts set out detailed rules on personal data in the Armed Forces, including MUST and FRA.[34] Under section 10 of the Signals Intelligence Act, SIUN can order that a signals collection operation be stopped and require deletion of whatever data has been collected. This has (so far) only happened once, in 2019. Signals intelligence is a very technical area. Until recently, SIUN did not have any technical expertise of its own to draw upon, and was thus heavily dependent on FRA, the body it was supposed to be monitoring. SIUN is now in the process of employing its own technical expert(s).[35]

Finally, Sweden's data-protection authority has some overlapping competence with SIN and SIUN, as regards monitoring data files. The Authority for Privacy Protection (*Integritetsskyddsmyndigheten*, formerly the Data Inspectorate) has a general competence to monitor all public (and private) data banks for compliance with data protection principles, which means it also has the power to monitor personal data held by FRA, MUST, and the Security Service. This overlap in oversight competence is not optimal, as it means a certain duplication of work.

V. RELEVANT LAW

The statutory provisions covering the collection process have been largely set out in the preceding section. This section will cover the overarching constitutional and treaty-law framework, and the issue of how to make these rules a natural part of the work of the agencies.

The Swedish constitution protects "against body searches, house searches and other such invasions of privacy, against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications."[36] It further provides that "everyone shall be protected in their relations with the public institutions against significant invasions of their personal privacy, if these occur without their consent and involve the surveillance or systematic monitoring of the individual's personal circumstances."[37] That right is relative, however, meaning that it can be limited by statute. There is no irreducible core and absolute right of privacy.

The rights provided by IG 2:6 paragraph 2 are also comparatively new, dating from 2011. Historically, freedom of information and freedom of expression have been more strongly guaranteed than privacy and data protection. There is no express constitutional right to informational self-determination, though it can be seen as an implicit part of the right to personal integrity. The Freedom of the Press and Freedom of Expression Acts also have constitutional status, and these contain, inter alia, rights for everyone (including civil servants) to communicate official information to the press for the purpose of publication, except for limited categories of secret information, set out exhaustively in the Act on Transparency and Secrecy.[38]

These rights are not unlimited, however: limitations "may be imposed," but "only to satisfy a purpose acceptable in a democratic society.[39] The limitation must never go beyond what is necessary with regard to the purpose which occasioned it, nor may it be carried so far as to constitute a threat to the free shaping of opinion as one of the fundaments of democracy. No limitation may be imposed solely on grounds of a political, religious, cultural, or other such opinion."

The constitutional protection of privacy applies to non-Swedish citizens present in Sweden, although it is possible, by statute, to provide for a lower level of protection.

A further level of rights protection is provided by the European Convention on Human Rights (ECHR),[40] which is incorporated into Swedish law. The ECHR has quasi-constitutional status and applies to "everyone" within a state's jurisdiction, regardless of nationality.

The EU Court of Justice, despite the exclusion of issues of national security from the scope of the Treaty on European Union (Article 4) has taken the view that metadata collection and retention, even for national security purposes, can fall within EU jurisdiction.[41] A consequence of this is that the rights protections (privacy, data protection etc.) provided by the EU Charter on Fundamental Rights and Freedoms would apply to these activities (see further below, section VII).

The Swedish constitution protects "against body searches, house searches and other such invasions of privacy, against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications.

Sweden appears to have (apart from ships and planes in and above international waters in the Baltic) relatively little extraterritorial collection of intelligence. However, to the extent that this occurs, it would be regarded as falling within national jurisdiction, and thus subject to constitutional and ECHR protections.[42] Bearing in mind the routing of internet cables, Sweden will undoubtedly be acquiring and processing personal data of certain individuals subject to targeting orders, e.g. in Russia.

Sweden allows non-residents to complain to SIUN and such cases have been filed. However, non-resident foreigners are likely to receive the same bland information as citizens and resident foreigners: namely, that SIUN has investigated the allegation and found no violation of the law. The value of this is that an objective body has investigated and found either

that FRA has no data on the person in question, or that it has such personal data, but (much less likely) the acquisition, retention, and communication of this data has been lawfully authorised by a targeting order. This is likely to provide little reassurance for most people (at least, most people likely to complain).

Conceding a right to complain has—so far—not led to SIUN being deluged in complaints. Nor does it mean that non-resident foreigners are regarded as having the same privacy rights as Swedish citizens and resident foreigners: in particular, the communication of this data to foreign partners is likely to be easier, as there is less likely that there would be countervailing "Swedish interests" to take into account.

The reality of implementing these rules is more complicated. There are several well-known difficulties and risks in overseeing intelligence agencies. "Capture" of the oversight body is one of these, as the intelligence agency will likely have a monopoly, or near monopoly, of information on methods. An intelligence agency which is under political pressure to produce results is likely to be more willing to "steer close to the wind" and stretch its interpretation of applicable legislation. This is also a risk where legislation is framed in broad, technique-neutral terms, constant technological innovation and development can mean that mean that more can be done within the existing legal framework. Interpretative "primacy" can be conceded to the agency, where there is little prospect of judicial scrutiny.

Domestic electronic surveillance operations are controlled principally by the authorisation process. This process requires the Security Service to first to convince a specialist prosecutor that a given security offence is being committed. The prosecutor must then convince a court of the necessity and proportionality of the operation. The post-hoc oversight by SIN is mainly a back-up to this authorisation process. Because interception of communications (and even more so, bugging or equipment interference) consumes time and resources, the Security Service and the prosecutor have a strong interest in efficiency. This should in turn have the effect of minimizing abuse/over-use.

Foreign intelligence surveillance, by comparison, lacks a comparably clear legal framework. Moreover, the available technology permits the collection of vast amounts of data. The permitted grounds for collecting signals intelligence provide some safeguards (e.g., against using signals intelligence to gather economic intelligence for the benefit of companies) but these grounds must, of necessity be framed in relatively general terms. For example, it must be possible to gather intelligence on companies where there are good grounds for suspecting sanctions or export control violations.

Automated search terms need to be framed tightly so as to minimize risks for personal integrity. Laws are often framed in terms of setting limits, together with the need to make an individual-case-oriented proportionality assessment. Technology by contrast is often designed to maximize results. To attempt to bridge this gap between lawyers and engineers, FRA has an "integrity advisory body"[43] which meets periodically to examine how legal rules are "translated" into algorithms.

Information collected, processed, and retained on individuals is a particular focus for Swedish safeguards and oversight processes. The SIUN, which oversees foreign intelligence, has a specific mandate to examine any such information, which must always be justifiable under a specific tasking directive. Under section 7 of the Signals Intelligence Act, intercepted data must be destroyed immediately by the FRA if it (i) concerns a specific natural person and lacks importance for the signals intelligence,[44] (ii) is protected by constitutional provisions on secrecy for the protection of anonymous authors and media sources (see further below), (iii) contains information shared between a suspect and his or her legal counsel and is thus protected by attorney-client privilege, or (iv) involves information given in a religious context of confession or individual counselling, unless there are exceptional reasons for

examining the information.

SIUN has this as part of its ex officio competence, and a complaints procedure provides an added incentive to monitor the area.[45] While this is a useful part of the control system (and required by the ECHR), the value of this from the individual's perspective is limited. The individual receives no explanations or information beyond the fact that SIUN has investigated the complaint and found no violation of the law.[46]

VI. TRANSPARENCY

The relevant laws governing national-security surveillance for foreign intelligence are publicly available. The procedures are described in some detail in the preparatory legislative works, which have a high status as a legal source in the Swedish legal tradition. Information on policies and investigations made by SIUN is not generally made available. Somewhat more information can be found in the annual reports the government makes to the parliament,[47] and in the annual reports published by SIUN and the Authority for Privacy Protection. FRA "responds" to SIUN investigations by noting which of these resulted in changes in procedure etc., without going into details. Little statistical information is provided; for example, the reports do not break out the number of complaints which were and were not well founded.

For domestic national security surveillance, the police and Security Service are required to report statistics every year to the Prosecutorial Authority, which produces a public report the following year.[48] Security Service statistics are aggregated for secrecy reasons. Disaggregated statistics are reported to SIN, but not made public.

VII. REFORMS

In recent years, Swedish law has been updated to authorize new types of surveillance, such as equipment interference. Most reforms being discussed now relate to increased powers to deal with organized crime, not national security. Reforms related to foreign intelligence have been made recently to the law governing handling of personal data by FRA[49] and MUST.[50] The speed of technological development is great, and modernisation of the law is needed to keep up.

The judgment of the ECtHR in Centrum för *rättvisa v. Sweden* has triggered additional minor reforms.[51] The ECtHR broadly held that the Swedish system was acceptable.[52] However, the court also criticised SIUN's dual supervisory-complaints role and the lack of a clear and specific requirement to consider privacy interests of individuals when transferring intelligence to foreign partners. A commission of inquiry is considering reform of the law, including how it can best be brought in line with the judgment.[53] It is at present unclear whether legal reform will also be necessary to bring Swedish law in line with EU law. This hinges on whether FRA's methods for acquisition of metadata (the mirroring of cable traffic which is channelled through internet choke points when it enters and leaves Swedish territory) is seen as imposing "processing" requirements on telecommunication companies.[54]

VIII. CONCLUDING REMARKS

The Swedish legal frameworks for approving and overseeing domestic and foreign electronic intelligence collection appear to be relatively strong when compared with those in other democratic states. However, in this area, practice is at least as important as the wording of the law. The actual amount of Swedish intelligence collection can be assumed to be small in comparison to the big actors in the field, and this naturally limits the potential for abuse of power. It is nonetheless necessary that the oversight bodies possess a residual independent investigative capacity. In this respect SIUN's recent decision to employ technical expertise is good, though overdue.

Both the "domestic" and "foreign" oversight bodies are small, and thus vulnerable to serious loss of "institutional memory" if any of the small permanent staff leave. With the intermingling of "foreign" and "domestic" threats, it seems increasingly difficult to justify parallel oversight systems. Still, it is unlikely that this will be changed.

Assuming that the EU Court of Justice does not make further assertions of competence to regulate this field, oversight issues are unlikely to be at the forefront of the Swedish debate in the next few years, even if Sweden as a state prides itself on its respect for "good governance" and international human rights standards. The – belated – political realization of the very real security threats posed to Western states by Russia and China in particular, together with impending Swedish membership of NATO, mean that effectiveness and efficiency in intelligence collection are likely to be most important.

ENDNOTES

1. Frederick Wallin, *A Brief History of the FRA*, https://www.fra.se/omfra.4.6a76c4041614726b25ac2.html.
2. *See Sakhertpolisen*, ORGANISATION (Jun. 16, 2023), https://sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/about-the-security-service/organisation.html (accessed Jun. 16, 2023)
3. Defence Intelligence Act (2000:130) section 4 provides "Within the defense intelligence activities, no measures may be taken that aim to solve tasks that according to laws or other regulations are within the framework of the Police Authority, the Security Service and other authorities' law enforcement and crime prevention activities. If there are no obstacles in accordance with other regulations, however, the authorities that conduct defense intelligence activities may provide support to other authorities' law enforcement and crime prevention activities."
4. Signals Intelligence Act, section 2.
5. Signals Intelligence Act, section 2a.
6. Bill 2006/07:63, p. 43.
7. Governed by Code of Judicial Procedure (CJP) 23:1.
8. This is specifically provided for in the Act Prohibiting the Use of Defence Intelligence in Investigating Crime (2019:547).
9. CJP 27:20
10. For the *travaux préparatoires* see Bill 2011/12:55, p. 130. It has recently been proposed that wiretapping (i.e. interception of content of communications) , as well as the use of trojans should also be allowed to identify a suspect where this is of particular importance to the investigation (SOU 2022:19).
11. There is no exhaustive definition of the concept in law. In doctrine, it means the exercise of authority that involves an intrusion into a person's property or personal integrity without consent, both physical investigative powers (arrest, search and seizure etc.) as well as secret investigative powers (wiretapping, etc.), Gunnel Lindberg, Tvångsmedel, 2022, p. 47.
12. There is a proposal to extend the list of offences so as to cover more organised crime, SOU 2022:52.
13. Act 2022:666.
14. Act 2020:62.
15. Different courts of appeal refused the motions to dismiss this evidence, and the Supreme Court confirmed this approach indirectly when it refused leave to appeal this point.
16. CJP 27:21.
17. Act on the Collection of Data on Electronic Communications in Law Enforcement Intelligence (2012:278).
18. Act on Special Control of Aliens (2022:700), Chapter 5, section 1.
19. Although SIN's mandate is only framed in terms of ensuring compliance with the law, a proportionality test is a fundamental part of this. These laws include the limits set out on sensitive data in the Constitution (below), and in particular the Act (2019:1182) on the Security Service's handling of personal data, and the Act (2019:547) Prohibiting the Use of Defence Intelligence in Investigating Crime.
20. Act on the Supervision of Certain Crime Fighting Activities (2007:980)
21. These eight purposes are elaborated upon in the preparatory works to the legislation (Bill 2008/09:201, pp. 108-109).
22. Id.
23. The Government Offices include the Prime Minister's Office, the ministries, and the Office for Administrative Affairs.
24. Foreign Intelligence Ordinance (*Förordningen om försvarsunderrättelseverksamhet*; 2000:131), section 2a.
25. This obligation is in the Act on Electronic Communication (2003:389), Chapter 6 section 19 a.
26. The preparatory (Bill 2006/07:63, p. 90) notes that the use of search terms that are attributable to a particular individual ("strong selectors"), such as personal names, telephone numbers, email, or IP addresses, involves special risks to individual privacy. Thus this should only be considered under special conditions and should be preceded by a thorough necessity assessment, notably as to whether the information which can thereby be obtained is of such importance that it justifies the measure.
27. FRA may collect electronic signals in order to monitor changes in the international signals environment, technical advances and signals protection and to develop the technology needed for signals intelligence (Signals Intelligence Act, section 1(3)).
28. FRA has to report to the court immediately and the court shall without delay decide in the matter. The court may revoke or amend the permit (section 5b).
29. As an additional control mechanism, it is SIUN which physically "switches on" FRA access to these.
30. Signals Intelligence Act, § 4a.
31. Signals Intelligence Act, § 5.
32. *Id.* § 5a. The ECtHR (see below, Part V) held that the extent of the oversight of the process was satisfactory (*Centrum för Rättvisa* para. 302). Nationality-based differences in the standard for authorization are discussed below.
33. Provisions on the court are found in Act 2009:966.

34. Acts 2021:1171 and 2021:1172 respectively.
35. SIUN, Annual Report for 2022, p. 13.
36. *See,* Instrument of Government (IG) 2:6 paragraph 1.
37. *Id.* at Section 2:6 paragraph 2.
38. Act on Transparency and Secrecy, 2009:400
39. *See,* IG 2:20.
40. Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI. 1950
41. For a discussion of these issues, see I Cameron, Metadata retention and national security: Privacy International and La Quadrature du Net, 58 Common Market Law Review 1433–1472 (2021).
42. This is the position of the European Court of Human Rights (ECtHR) in *Centrum för rättvisa v. Sweden,* Nr 35252/08, and *Big Brother Watch and others v. UK*, Nr. 58170/13, 13 September, both 25 May 2021 (Grand Chamber). The Swedish government has accepted this. See also below, VII.
43. The Integrity Advisory Body is provided for by statute in the Signals Intelligence Act. *See,* Signals Intelligence Act, Sec. 11.
44. The ECtHR (see below VII) took the view that the destruction requirement should be broader, not simply concerning information on individuals.
45. *See* Signals Intelligence Act, § 10a.
46. The lack of transparency in the complaints system was criticized by the ECtHR, see below VII.
47. For the latest, see 2022/23: FöU 5. See also the Commission of Inquiry Uppföljning av signalspaningslagen, SOU 2011:13, and the National Audit Office control of SIUN, Kontroll av försvarsunderrättelseverksamhet, Riksrevisionen (RiR) 2015:2.
48. he latest such report (for 2022) can be found at https://www.aklagare.se/globalassets/dokument/rapporter/arsrapporter/redovisning-av-anvandningen-av-vissa-hemliga-tvangsmedel-under-2022.pdf.
49. Försvarets radioanstalts internationella samarbete – en översyn av regelverket (SOU 2020:68), led to Regeringens proposition 2020/21:224 Behandling av personuppgifter vid Försvarsmakten och Försvarets radioanstalt and, as already mentioned, a new Act (2021:1172). Further minor amendments can be expected as a result of the Centrum för Rättvisa case (below, this section).
50. *See supra* part IV.
51. *See supra* part VII.
52. The ECtHR now insists that there be an independent authorizing body. *See* Big Brother Watch v. UK, Nos. 58170/13, 62322/14, and 24960/15 (25 May 2021). However, Swedish legislators anticipated this and, as already noted, created such a body (FUD) in 2008 when they reformed the control/oversight system.
53. Dir. 2022:120).
54. Case C 623/17, Privacy International EU:C:2020:790 and Joined Cases C 511/18, C 512/18 and C 520/18, La Quadrature du Net and Others v Premier ministre and Others, EU:C:2020:791. For analysis, see Cameron, supra note 46.