PRIVACY INTERNATIONAL

Human Rights Committee 116th Session

The Right to Privacy in Sweden

Submitted by Privacy International, Civil Rights Defenders and DFRI in advance of the consideration of the periodic report of Sweden, Human Rights Committee

March 2016


PRIVACY
INTERNATIONAL


:DFRI
Föreningen för digitala fri- och rättigheter


CIVIL
RIGHTS
DEFENDERS

1. Introductions

Privacy International, Civil Rights Defenders and DFRI note Sweden's written replies to the list of issues in relation to Swedish laws, policies and practices on interception of personal communications.[1]

The following comments are based on the analysis of the Swedish legislation, as well as policies and practices on surveillance by Privacy International, Civil Rights Defenders and DFRI.[2]

Since the Human Rights Committee's last consideration of Sweden in 2009, when it expressed concerns about the "wide powers of surveillance in respect of electronic communications" granted under the Act on Signals Intelligence in Defence Intelligence Operations, other UN and regional bodies have made recommendations to review and reform the Swedish surveillance law to bring into compliance with international human rights standards.[3] So far Sweden has failed to effectively address these recommendations, as this briefing illustrates.

2. Mass surveillance capacity of the FRA

With the enactment of Act [2008:717] on Signals Intelligence in Defence Intelligence Operations [hereinafter the Surveillance Act], the National Defence Radio Establishment [Försvarets Radioanstalt – FRA] was granted a mandate to collect data from transnational telecommunications cables for the first time. Apprehensions that the FRA would engage in mass, suspicionless surveillance were raised and subsequently validated through international disclosures.[4]

Under the Surveillance Act, the collection of foreign communications [SIGINT] must be automated and restricted to "signals identified through search terms [sökbegrepp]". The FRA must "formulate and apply search terms with respect for individual integrity" so that the impact of operations is limited.[5] However, revelations concerning Five Eyes SIGINT collection practices raise serious doubts about the way modern SIGINT collection can target on communications, instead suggesting a high degree of arbitrariness. Analysis of the programs shows that merely 5 percent of automatically analysed data is of "definite interest" to search terms, and only 20 percent of the data is of "high" or "definite relevance" when manual analysis is initiated.[6]

So far, the Swedish Government has not provided sufficient reassurances that FRA collection of foreign communications is accurate, targeted, and thereby

1 UN doc. CCPR/C/SWE/7, 24 July 2015.

2 Privacy International is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. Civil Rights Defenders is an independent expert organisation founded in Stockholm in 1982 with the aim of defending human rights, in particular people's civil and political rights, while also supporting and empowering human rights defenders at risk. DFRI is a Swedish non-profit and non-party organisation working for digital rights.

3 See Human Rights Committee, Concluding observations on the sixth periodic report of Sweden, UN doc. CCPR/C/SWE/CO/6, 7 May 2009; Recommendations contained in the second UN UPR Cycle (UN doc. A/HRC/29/13, 13 April 2015, see the recommendations of Slovenia and the Netherlands. Available at: http://www.upr-info.org/sites/default/files/document/sweden/session_21_-_january_2015/a_hrc_29_13_e.pdf). See also findings in report commission by the European Parliament (2013): http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf

4 Magnus Sandelin (2013), Läs dokumenten om Sverige från Edward Snowden. Available: http://www.svt.se/ug/las-dokumenten-om-sverige-fran-edward-snowden. Last accessed 12/18/2015.

5 Clause 3 § Act (2008:717) on Signals Intelligence in Defence Operations.

6 Erik Zouave, Computers vs humans: Why there's no difference between who, or what, looks at your data. Available: https://www.privacyinternational.org/node/486. Last accessed 18/12/2015; National Security Agency SIGINT Development (2012), Identifier Lead Triage. Available: https://www.aclu.org/files/natsec/nsa/ghostmachine-identifier-lead-triage-with-echobase.pdf. Last accessed 18/12/2015.

compliant with Article 17 under the International Covenant on Civil and Political Rights.

Instead, concerns about the capacity of FRA to carry out mass surveillance emerged in the past few years.

Disclosures on the FRA and Five Eyes give detailed insight into the technical realities of personal data processing ["behandling"][7] within the FRA.[8] According to documents released in the last couple of years, the Swedish intelligence agency is a user of XKEYSCORE.[9] The program collates information gathered through ether, cable, and Computer Network Exploitation [see more below], and facilitates analysis of data through automated and manual processes. XKEYSCORE provides access to data in bulk, not only on the basis of targeted and limited identifiers such as IP and e-mail addresses, but through sweeping selectors such as website visitor logs.[10] Intelligence officers, including in Sweden, can access swathes of personal data on the premise of imprecise justifications, such as "extremism" or "terrorism."[11]

3. Discriminatory regime in the Surveillance Act

The Surveillance Act creates a regime of surveillance that is discriminatory on the basis nationality. The FRA is prohibited from the collection of signals that have both a sender and a recipient located in Sweden and must destroy those signals once identified.[12] Collection of data with both a Swedish sender and recipient are, under most circumstances, restricted to criminal investigations and require "reasonable suspicion" of serious offenses[13] thereby providing higher safeguards and protection than the collection of foreign communications under the Surveillance Act. Because Swedish citizens are more likely to be present in Sweden, the Surveillance Act is therefore likely to have a disparate adverse impact on the privacy of non-Swedish persons.

The UN High Commissioner for Human Rights and the UN Special Rapporteur on counter-terrorism and human rights have noted how several legal regimes on interception of personal communications, like the Swedish one, distinguish between obligations owed to nationals and non-nationals and residents and non-residents, providing external communications with lower or non-existent protection, in ways that are discriminatory and incompatible with Article 26 of the ICCPR.[14] The UN Special Rapporteur on counter-terrorism concluded

7 See 4§ Act (2009: 259) on the processing of personal data in the National Defence Radio Establishment defence intelligence and development activities, definition of "behandling."
8 Magnus Sandelin (2013).
9 See NSA/CSSM (2013) Visit Précis: SWEDUSA 2013 Strategic Planning Conference (SPC). Available: https://www.documentcloud.org/documents/894387-se-xkeyscore-ingvar-akesson-dirnsa-meeting-2013.html Last accessed 18/12/2015.
10 Glenn Greenwald, XKeyscore: NSA tool collects 'nearly everything a user does on the internet', 2013. Available: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. Last accessed 18/12/2015.
11 Electronic Frontier Foundation. (n.d.). 20131211-SVT-Xkeyscore Slide with Swedish Example. Available: https://www.eff.org/document/20131211-svt-xkeyscore-slide-swedish-example. Last accessed 18/12/2015.
12 2 and 2a §§ Act (2008:717) on Signals Intelligence in Defence Operations.
13 SOU 2009:66 Signalspaning för polisiära behov (Statens Offentliga Utredningar, Stockholm 2009); See also: Proposition (2015:16/78) Ett särskilt straffansvar för resor i terrorismsyfte (Swedish Government, 17 December 2015) Available http://www.regeringen.se/rattsdokument/proposition/2015/12/prop.-20151678/ Last accessed 15/01/2016.
14 See report of the UN High Commissioner on Human Rights on the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014; and report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014.

that states "are legally bound to afford the same protection to nationals and non-nationals, and to those within and outside their jurisdiction".[15] Similarly this Committee has consistently recommended that any interference with the right to privacy in the context of communications surveillance complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance.[16]

Further the distinction is arbitrary and rendered meaningless in the context of the technical architecture of modern digital communications, with messages such as e-mails routed through different countries even if both the sender and the intended recipient are resident in Sweden.

In fact, both the Swedish Data Protection Authority and the Post and Telecom Authority have also expressed misgivings on the technical feasibility of sifting out domestic data.[17] In June 2015 it has been revealed that communications via services such as Google and Facebook, relying on foreign servers, also constitute foreign communications.18 As a result a very small portion of everyday communications are thus beyond the FRA's reach. Repeated critique from domestic oversight brings FRA data processing procedures and policies into question.[19]

4. Intelligence sharing without accessible legal basis

The FRA is a third party to Five Eyes international signals intelligence (SIGINT) network.[20] Third Party partnerships imply not just an exchange of finished intelligence reports but joint operations and analysis involving the trade of technologies and access to bulk data, either filtered, or increasingly in its raw unfiltered form.

Despite this level of cooperation, Swedish legislation regulating intelligence sharing with foreign intelligence agencies is opaque and lays down a remit for cooperation and information-sharing only limited by need to conduct collaboration in the "interest of the Swedish Government" and national security.[21]

15 Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, paragraph 43.

16 See, for example, Human Rights Committee, Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland, UN doc. CCPR/C/GBR/CO/7, 17 August 2015.

17 Datainspektionen (2010) Datainspektionens redovisning av regeringsuppdraget. (Fö2009/355/SUND, 2010-12-06). Available http://www.datainspektionen.se/Documents/beslut/2010-12-07-fra.pdf Last accessed 14/01/2016; Stefan Winiger. (2009). Tung kritik mot FRA:s internetspaning. Available: http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=2658657. Last accessed 14/01/2016.

18 Svensk Signalspaning under 70 År 2015. Youtube video, Försvarspolitisk Arena (Almedalen, Gotland: 30 June, 2015) Available at: https://www.youtube.com/watch?v=cmuapzsQNSk Last accessed: 16/07/2015.

19 Datainspektionen (2010) Datainspektionens redovisning av regeringsuppdraget. (Fö2009/355/SUND, 2010-12-06). Available http://www.datainspektionen.se/Documents/beslut/2010-12-07-fra.pdf Last accessed 14/01/2016. Anna Persson. (2013). FRA lagrade känsliga personuppgifter olagligt – prickas för andra gången i år. Available: http://www.dagensjuridik.se/2013/06/fra-lagrade-kansliga-personuppgifter-olagligt-prickas-andra-gangen-i-ar. Last accessed 14/01/2016; Dagens Juridik. (2014). Fredrick Federley riktar allvarlig kritik mot FRA – "klarar man inte detta får vi se över lagen". Available: http://www.dagensjuridik.se/2014/04/fredrick-federley-riktar-allvarlig-kritik-mot-fra-klarar-man-inte-detta-kommer-vi-att-fa-se-. Last accessed 14/01/2016.

20 Magnus Sandelin (2013); Electrospaces. (2013). 14-Eyes are 3rd Party partners forming the SIGINT Seniors Europe. Available: http://electrospaces.blogspot.se/2013/12/14-eyes-are-3rd-party-partners-forming.html. Last accessed 18/12/2015.

21 9§ Act (2008:717); 3§ Act (2000:130) on Defence Intelligence Operations; 6§ Regulation (2008:923) On Signals Intelligence in Defence Intelligence Operations; 17§ Act (2007:259) on Treatment of Personal Data in the National Defence Radio Establishment's Defence Intelligence and Development Operations.

As such, the domestic legal regime fails to meet the requirement of the quality of the law necessary to comply with Article 17 of the International Covenant on Civil and Political Rights. As noted by the High Commissioner for Human Rights in her report on the right to privacy in the digital age summarising the findings of international human rights bodies, including this Committee, interferences with the right to privacy must be executed under laws that are "sufficiently accessible, clear and precise so that an individual may… ascertain who is authorized to conduct data surveillance and under what circumstances."[22]

5. Computer Network Exploitation (hacking)

The FRA rely on collaboration with foreign intelligence agencies to develop Computer Network Exploitation [CNE] or "active signals intelligence" ["aktiv signalspaning"], despite lacking a clear and accessible mandate to do so under the law.[23] The FRA has developed its own CNE program, WINTERLIGHT,[24] as part of the NSA QUANTUM program,[25] described as the "NSA's most powerful internet attack tool."[26] In the wake of these disclosures regarding the use of CNE by Swedish authorities, the Director of the Swedish Defence Intelligence Court clarified, upon request, that "the law [i.e. the Surveillance Act] is not hinged on methods other than to differentiate between ether and cable."[27]

In a recent proposal on counterterrorism legislation, the Swedish Government is considering extending powers of CNE to the Security Service [Säkerhetspolisen – Säpo], the Police and Customs, through a new "coercive measure" ["tvångsingrepp"] called "data scanning" ["dataavläsning"].[28] If the bill is passed, Säpo may be mandated to develop or purchase its own CNE platforms, or receive information from FRA CNE operations. As the FRA is responsible for aiding other national authorities in the evaluation, development, and acquisition of signals intelligence systems,[29] and national law enforcement currently lacks independent signals intelligence capacity it is likely that law enforcement will be able to direct the FRA's CNE.[30] Sweden would thus be legislating for a transfer of technical capabilities from the FRA that are currently neither confirmed nor denied. Additionally, the Government has yet to propose how CNE would be applied, whether as a method of investigations under "reasonable suspicion," for preventive investigations under substantially lower thresholds, or under a SIGINT paradigm permitting untargeted use.[31]

22 Report of the Office of the United Nations High Commissioner for Human Rights, UN Doc. A/HRC/27/37, paragraph 23.

23 Thomas Oneborg (2013), Felaktigheter skadar svensk signalspaning. Available: http://www.svd.se/felaktigheter-skadar-svensk-signalspaning. Last accessed 16/07/2015; Johan Sigholm, (2013), "Nödvändig signalspaning". Available: http://www.fhs.se/nyteknik13. Last accessed 16/07/2015; Gunnar Rensfeldt, (2013), FRA hackar datorer - topphemligt projekt med NSA. Available: http://www.svt.se/ug/fra-hackar-datorer. Last accessed 16/07/2015.

24 NSA/CSSM (2013) Agenda: As of 23 April //1000 (NSA/CSSM 1-52: 20070108) Available at: https://www.documentcloud.org/documents/894403-finalagendaswedusa.html Last Accessed 16/07/2015; NSA/CSSM (2013) Visit Precis: SWEDUSA 2013 STRATEGIC PLANNING CONFERENCE (NSA/CSSM 1-52: 20070108) Available at: https://www.documentcloud.org/documents/894387-se-xkeyscore-ingvar-akesson-dirnsa-meeting-2013.html Last accessed 16/07/2015.

25 NSA/CSSM (2013) Agenda: As of 23 April //1000 (NSA/CSSM 1-52: 20070108) p. 2 Available at: https://www.documentcloud.org/documents/894403-finalagendaswedusa.html Last Accessed 16/07/2015.

26 Nicholas Weaver. (2014). A Close Look at the NSA's Most Powerful Internet Attack Tool. Available: http://www.wired.com/2014/03/quantum/. Last accessed 16/07/2015.

27 Uppdrag Granskning, (2013) Domaren: "Alla metoder är tillåtna". Available: http://www.svt.se/ug/blogg/domaren-alla-metoder-ar-tillatna. Last accessed 22/06/2015.

28 SOU 2015:63 Straffrättsliga åtgärder mot terrorismresor, p. 181 §1. Available at: http://data.riksdagen.se/fil/91DC5DC3-4F23-4176-814E-B11FC4EDB4F6. Last accessed 22/06/2015.

29 2 and 3 §§ Regulation (2007:937) with Instructions for the National Defence Defence Radio Establishment.

30 Proposition 2011/12:179 Polisens tillgång till Signalspaning i Försvarsunderrättelseverksamhet, Sections 4, 6 and 7. Available at: http://www.regeringen.se/rattsdokument/proposition/2012/09/prop.-201112179/ Last accessed 22/06/2015; Government Report (SOU) 2009:66 on Signals Intelligence for Police Purposes.

31 Proposition (2015:16/78) Ett särskilt straffansvar för resor i terrorismsyfte (Swedish Government, 17 December 2015) Available http://www.regeringen.se/rattsdokument/proposition/2015/12/prop.-20151678/ Last accessed 15/01/2016.

Computer network exploitation, or hacking, is an extremely intrusive form of surveillance. It can yield information sufficient to build a total profile of a person, from their daily movements to their most intimate thoughts. It is potentially far more probing than other surveillance techniques. Unlike intercept capabilities, hacking capabilities can be deployed in any number of configurations to do any number of different things. The logging of keystrokes, tracking of locations, covert photography, and video recording of the user and those around them enables intelligence agencies and the police to conduct real-time surveillance, while access to stored data enables analysis of a user's movements for a lengthy period prior to the search, access to saved documents and notes, draft messages and emails, and more. As such the use of CNE carries the potential to covertly build a significantly comprehensive picture on a user's private life. The Swedish Bar Association has criticized CNE for its severe impingement on human rights.[32]

The UN Special Rapporteur on freedom of expression expressed his concerns over such offensive spyware and stated that "[F]rom a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter –inadvertently or purposefully- the information contained therein. This threatens not only the right to privacy and procedural fairness rights with respect to the use of such evidence in legal proceedings."[33]

6. Inadequate Oversight

The State Inspection for Defence Intelligence [Siun] is the primary organ for the oversight of defence intelligence and related data protection laws, and all collection is authorized by Court Order from the Defence Intelligence Court [UNDOM].[34] Both mechanisms have been criticized by the European Parliament as lacking in independence.[35] Compliance with the Surveillance Act is also subject to annual review from the Swedish Government and Department of Defence.[36]
Subsequent to international disclosures on the Five Eyes, oversight bodies in some concerned states initiated detailed inquiries and published reports on international collaboration, adherence to domestic laws and surveillance practices.[37]

Siun has so far failed to meaningfully investigate the reports of intelligence sharing and FRA mass surveillance. It addressed the international cooperation in two short and sweeping sentences, without any mention of the disclosures or

32 Advokatsamfundet. (2014). SÄPO OCH ÅKLAGARE VILL PLANTERA "SPIONTROJANER" I DATORER. Available: https://www.advokatsamfundet.se/Nyhetsarkiv/2014/april/Sapo-och-aklagare-vill-plantera-spiontrojaner-i-datorer/. Last accessed 28/09/2015.
33 Report of UN Special Rapporteur on Freedom of Expression and Opinion, A/HRC/23/40, 17 April 2013, para. 62.
34 Statens inspektion för försvarsunderrättelseverksamheten. (n.d.).Siun. Available: http://www.siun.se/. Last accessed 14/01/2016.
35 European parliament Directorate General for Internal Policies (2013) National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law (PE 493.032), 26. Available http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf Last accessed 04-02-2016
36 Regeringen (2014) Integritetsskydd vid Signalsspaning i Försvarsunderrättelseverksamhet (Regeringens Skrivelse 2014/15:27 Available http://www.regeringen.se/contentassets/a2912ffa4aaf40ddbeb5fdff9ae3d34a/skr.-20141527-integritetsskydd-vid-signalspaning-i-forsvarsunderrattelseverksamhet Last accessed 14/01/2016.
37 For the UK, see Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework (2015); Independent Reviewer on counter-terrorism legislation, A question of trust (2015); for the Netherlands, see Investigations into the compliance of the General Intelligence and Security and the Military Intelligence and Security Resolutions, The Review Committee for the Intelligence and Security Services (2015); for Germany, see ad-hoc inquiry of the Bundestag into the "NSA Affair".

serious allegations stemming from them. It did this only to assert that it had no complaints on the matter.[38] On the basis of this inadequate review, the Swedish Government published an equally sweeping three-page report.[39] It also initiated Parliamentary deliberations on the intelligence cooperation with the Five Eyes, only to issue the blanket statement that "the system to protect privacy during signals intelligence works in the manner intended by the law."[40]

The Data Protection Authority (DI) can also oversee FRA registration and processing of data on the basis of anonymous complaints or referrals from Siun inquiries. In December 2015, the DI initiated an inquiry into the FRA based on a Siun referral. However, neither the matter under review nor the initial Siun findings have been made public.[41]

7. Recommendations

Based on these observations, Privacy International, Civil Rights Defenders and DFRI suggest the following recommendations for the Swedish government:

- Take all necessary measures to ensure that its surveillance activities, both within and outside Sweden, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under surveillance, which includes refraining from engaging in mass surveillance;

- Review and reform the Surveillance Act in order to ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that: (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance, and procedures for the use and storage of data collected; and (iv) provide for effective safeguards against abuse;

- Review the practice of intelligence sharing with foreign agencies to ensure its compliance with the right to privacy, under Article 17 of the Covenant.

38 Statens Inspektion för Försvarsunderrättelseverksamheten (2014) Årsredovisning 2013 (13-2014Ö:1, 2014/02/19) Available http://www.siun.se/dokument/Arsredovisning_2013.pdf Last accessed 14/01/2016.

39 Regeringen (2014) Integritetsskydd vid Signalsspaning i Försvarsunderrättelseverksamhet (Regeringens Skrivelse 2014/15:27 Available http://www.regeringen.se/contentassets/a2912ffa4aaf40ddbeb5fdff9ae3d34a/skr.-20141527-integritetsskydd-vid-signalspaning-i-forsvarsunderrattelseverksamhet Last accessed 14/01/2016.

40 Sveriges Riksdag (2015), Debatt och Beslut: Integritetsskydd vid signalspaning i försvarsunderrättelseverksamhet. Available: http://www.riksdagen.se/sv/Debatter--beslut/Debatter-och-beslut-om-forslag/Arendedebatter/?did=H201F%C3%B6U5&tab=2#/panel2. Last accessed 14/01/2016.

41 Dagens Juridik. (2015). Hemligt varför DI granskar FRA efter viss "observation" från annan myndighet. Available: http://www.dagensjuridik.se/2015/12/hemligt-varfor-di-granskar-fra-efter-viss-observation-fran-annan-myndighet. Last accessed 04/02/2016.

- Publicly avow the surveillance technologies capacities, such as Computer Network Exploitation (CNE), and assess whether CNE can be used at all in a manner that is necessary and proportionate. If the CNE power is to be retained, it should only be deployed in the most compelling and narrowly-defined circumstances, with the greatest oversight and safeguards.

- Reform the current oversight system of surveillance activities to ensure its effectiveness;

- Ensure that affected persons have access to effective remedies in cases of abuse.