
# The Right to Privacy in Sweden

## Stakeholder Report Universal Periodic Review 21st Session - Sweden

**Submitted by Privacy International**
**June 2014**

## Introduction

This stakeholder report is a submission by Privacy International (PI). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. PI wishes to bring concerns about the protection and promotion of the right to privacy in Sweden before the Human Rights Council for consideration in Sweden's upcoming review.

## The right to privacy

Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from arbitrary State intervention and from excessive unsolicited intervention by other uninvited individuals.[2] Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[3]

As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[4]

---

[1] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

[2] Martin Scheinin, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 2009, A/HRC/17/34.

[3] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[4] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

A number of international instruments enshrine data protection principles,[5] and many domestic legislatures have incorporated such principles into national law.[6]

**Follow up to the previous UPR**

In its national report for the first UPR cycle, Sweden observed:

> The increased international attention given during the last few years to the fight against terrorism and organised crime has highlighted the challenge in ensuring full respect for human rights, including freedom of expression and the right to privacy, in countering such crimes. The combined effect of all secret investigative measures, for example, must be weighed against the consequences that the measures taken together will have for privacy and the rule of law. There can be no question of augmented powers unless such powers are combined with clear rules for their exercise in conformity with international obligations, as well as for mechanisms for thorough scrutiny of the way they have been exercised afterwards.

One of the recommendations that came out of Sweden's review in 2010 was "to closely monitor the interpretation and application of the 2008 Surveillance [Signals Intelligence] Act to prevent any interference with the right to privacy". In its national responses, Sweden "noted that there was a legitimate interest in having an efficient tool for collecting intelligence from foreign counties, balanced with the protection of personal integrity and the right to privacy" and "stressed that its primary interest was in creating a clear legal basis for such activities, which was in conformity with its human rights obligations."

**Domestic laws related to privacy**

Sweden's Constitution consists of four elements: the Instrument of Government, the Act of Succession, the Freedom of the Press Act, and the Fundamental Law on Freedom of Expression. These contain several provisions relevant to the right to privacy.

---

[5] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

[6] As of December 2013, 101 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

For example, **Article 2 of Chapter 1 of the Instrument of Government** includes:

> The public institutions shall promote the ideals of democracy as guidelines in all sectors of society and protect the private and family lives of the individual.

**Article 6 of Chapter 2** provides:

> Everyone shall be protected in their relations with the public institutions against any physical violation also in cases other than cases under [the relevant articles]. Everyone shall likewise be protected 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.

Other laws relating to privacy include the **1998 Personal Data Act**, which applies to automatic processing of personal data by public or private entities and is supplemented by a variety of other laws in specific areas, and the **2008 Signals Intelligence Act**, which regulates interception of communications, alongside other legislation.

**Areas of concern**

Since June 2013, documents from NSA whistleblower Edward Snowden have revealed that Sweden's National Defence Radio Establishment (FRA) works with other European intelligence agencies and the National Security Agency (NSA) of the United States of America on a number of levels.[7] For example, the FRA has been a key partner to the NSA in intercepting the communications of Russian targets.[8] Most problematically, the FRA is implicated in mass surveillance practices; that is, the untargeted interception of communications on a massive scale.

Pursuant to the 2008 Signals Intelligence Act, the FRA collects communications travelling through fibre-optic cables that cross Sweden's borders. A 2013 Study by the Policy Department of the European Union Parliament[9] concluded that Sweden, along with several other EU countries, "may be running

---

[7] See, "NSA 'asking for' specific exchanges from FRA - Secret treaty since 1954", *Sveriges Television*, 8 December 2013, available at: http://www.svt.se/ug/nsafra4

[8] "Sweden key partner for U.S. spying on Russia: TV", *Reuters*, 5 December 2013 available at: http://www.reuters.com/article/2013/12/05/us-sweden-spying-idUSBRE9B40Q320131205

[9] European Parliament, Directorate General for Internal Policies, Policy Department C: Human Rights and Constitutional Affairs, *National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law: Study*, October 2013, available at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf

or developing [its] own large-scale internet interception programmes …, and collaborating with the NSA in the exchange of data"; these interception programmes were characterised by "[p]ractices of so-called 'upstreaming' (tapping directly into the communications infrastructure as a means to intercept data)". While the report did not consider Sweden's mass surveillance operations to be on the same scale as those of the NSA or its British equivalent, the Government Communications Headquarters (GCHQ), it did note that "operations and programmes for the mass collection of data by the FRA are reportedly elevating this agency to an increasingly important partner of the global intelligence network".

Additionally, the FRA is reportedly cooperating with the NSA in inserting malware on targeted computers, through an operation called "Winterlight": an internal NSA memo from April 2013 states, "FRA requested a WINTERLIGHT (Quantum project) update…" and notes that the US official should "[a]cknowledge the success that NSA, FRA … have had on WINTERLIGHT" at a meeting with the FRA.[10] The "Quantum" signifier refers to a project that targets specific users with the delivery of malware onto their machines and has leveraged an entire telecommunication company's network, Belgacom, to carry this out. The customers of Belgacom, a Belgian company, include the European Parliament and the European Commission.[11]

Beyond the practices of the FRA, the protection and promotion of the right to privacy has been undermined on multiple occasions since Sweden's first UPR review. Notable examples include:

- In early 2014, the website Lexbase was launched, offering access to the criminal records of what was said to be the whole Swedish population in a user-friendly and searchable interface. Although criminal records are publicly accessible according to Swedish legal principles, the launch and subsequent security breaches were harshly criticised by Swedish legal experts and privacy advocates.[12]
- In 2013, Swedish police were revealed to have developed a database of more than 4,000 Roma, illustrating family relationships among the group, in contravention of Swedish law.[13]

---

[10] "FRA part of top-secret hacker project", *Uppdrag Granskning*, 11 December 2013, available at: http://www.svt.se/ug/fra-part-of-top-secret-hacker-project

[11] Ibid.

[12] "Lexbase goes offline following hacker attack", *The Local*, 30 January 2014 available at: http://www.thelocal.se/20140130/lexbase-taken-offline-following-hacker-attack

[13] "Police database of Roma stirs outrage in Sweden", *Reuters*, 23 September 2013, available at: http://www.reuters.com/article/2013/09/23/us-sweden-roma-idUSBRE98M0EM20130923

- In 2013, the data silo company Logica uncovered a number of long-term security breaches of their systems. Intruders were found to have accessed a large range of sensitive information. Among the owners of the compromised data were the Swedish Tax Agency, the Police, the Collector's Office and other official bodies that had outsourced their data storage to Logica.[14]
- In 2013, press revelations showed how the Swedish Secret Service (Security Police) were trying to develop rapid procedures for retrieving data collected according to the European Data Retention Directive from Swedish operators. Among their strategies was to encourage Swedish internet service providers to outsource their data retention to third-party services, to license a special framework for easy access to collected data, and to pressure Swedish internet service providers to sign easy release agreements for customers' data.[15]
- In 2012, a Swedish investigative news programme, *Uppdrag Granskning*, reported that TeliSonora, a partially state-owned Swedish telecommunications company, was providing government authorities in Belarus, Uzbekistan, Azerbaijan, Tajikistan, Georgia and Kazakhstan with direct access to communications flowing through its networks, including text messages, phone calls, mobile location data and internet traffic.[16]
- Sweden does not have a sufficient export control regime in place to prevent the export of surveillance technology to repressive regimes. For example, until 2010, Swedish company Ericsson AB sold technology and equipment to Iran, which was used to target the communications of political dissidents.[17]

**Recommendations**

We recommend that the government of Sweden:

- Undertake an evaluation of its communications surveillance laws, policies and practices against the *International Principles for the Application of Human Rights to Communications Surveillance*;[18]

---

[14] Jonas Ryberg, "Så hackades Logica", 29 April 2013, available at http://computersweden.idg.se/2.2683/1.505012/sa-hackades-logica

[15] Monica Kleja, "IT & Telekom i samarbete med Telenor Företag", *NYTeknik,* 6 November 2013, available at: http://www.nyteknik.se/nyheter/it_telekom/allmant/article3784822.ece

[16] See, Eva Galperin, "Swedish Telcom Giant Teliasonera Caught Helping Authoritarian Regimes Spy on Their Citizens", *Electronic Frontier Foundation,* 18 May 2012, available at: https://www.eff.org/deeplinks/2012/05/swedish-telcom-giant-teliasonera-caught-helping-authoritarian-regimes-spy-its

[17] Ben Elgin, Vernon Silver and Alan Kat, "Iranian Police Seizing Dissidents Get Aid Of Western Companies", *Bloomberg,* 31 October 2011, available at: http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html

[18] https://en.necessaryandproportionate.org/text

- Commit to progressively implement reforms necessary to comply with the *International Principles*;

- Update its export control regulations to protect individuals abroad from abuses of surveillance technology.