PRIVACY INTERNATIONAL

Universal Periodic Review
Stakeholder Report: 21st Session, Turkey

The Right to Privacy in Turkey

Submitted by: Privacy International

‘No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.’

The Universal Declaration of Human Rights

PRIVACY INTERNATIONAL

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 Turkey before the Human Rights Council for consideration in Turkey'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] A number of international instruments enshrine data protection principles,[5] and many domestic legislatures have incorporated such principles into national law.[6]

---

[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).

[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),

Follow up to the previous UPR

Although Turkey's national report for the previous UPR noted that amendments to its Constitution had expanded "the scope and extent of the right … to privacy of individual life", no mention of privacy was made in the Working Group's Report. Additionally, despite illegal wiretapping scandals in Turkey in 2008 and 2009,[7] communications surveillance was not mentioned in the Working Group's report.

Domestic laws and regulations related to privacy

Article 20 of Turkey's **Constitution** protects the right to privacy and the right to data protection:

> Everyone has the right to demand respect for his/her private and family life. Privacy of private or family life shall not be violated.
>
> Unless there exists a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law, in cases where delay is prejudicial, again on the above-mentioned grounds, neither the person, nor the private papers, nor belongings of an individual shall be searched nor shall they be seized. …
>
> Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law.

Article 22 protects freedom of communication:

> Everyone has the freedom of communication. Privacy of communication is fundamental.
>
> Unless there exists a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law in cases where delay is prejudicial, again on the above-mentioned grounds, communication shall not be impeded nor its privacy be violated. …
>
> Public institutions and agencies where exceptions may be applied are prescribed in law.

---

available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

[7] h"Turkey: Freedom on the Net 2013", *Freedom House,* available at: http://www.freedomhouse.org/report/freedom-net/2013/turkey#.U5GR3V6VhEI

The Criminal Code contains provisions relating to privacy, including **Article 134**, which makes violating the secrecy of private life an offence punishable by imprisonment or a fine, and **Article 135**, which makes the unlawful recording of personal data an offence punishable by imprisonment. **Articles 136** and **138** offer additional protections for privacy. The Civil Code also contains provisions that protect the right to privacy.

Areas of concern

Lack of data protection legislation

A packet of constitutional amendments was approved by referendum in 2010. These included adding explicit recognition of the right to data protection to the Constitution. However, this constitutional protection for the right has not been appropriately supported by domestic legislation. While data protection issues are addressed in a number of pieces of legislation, Turkey has no specific data protection legislation and lacks a national data protection authority. A proposed law on data protection has been drafted, but has not yet been approved by the Turkish Parliament. This draft does not envisage the creation of an independent data protection authority.

The absence of data protection legislation permits rights-limiting practices to occur in Turkey. Examples include:

- In July 2012 it was revealed that Turkey's largest internet service provider had installed a service called "Phorm" on its networks. According to Freedom House, this behavioural advertising service "collects information on users' online behavior without their knowledge, performing deep-packet inspection (DPI) to essentially monitor a user's connection line and create a profile of the individual's online activities to then sell to advertisers".[8]
- The Department of Education created a "mobile portal" for students in primary and secondary education and their parents to receive information such as exam results; in 2012, personal information on 17 million students was sold to mobile network operators, which used the database for targeted advertising.[9]
- In 2013, the Ministry of Health reportedly established a centralised health record database without seeking patients' consent and sold information contained on the database to private companies.[10] Physicians raised significant concerns around the database and encroachment on patients' right to privacy.[11]

[8] "Turkey: Freedom on the Net 2013", *Freedom House,* available at: http://www.freedomhouse.org/report/freedom-net/2013/turkey#.U5GR3V6VhEI; see also, "Gizliliğinize dikilmiş bir çift göz", at http://enphormasyon.org/english.html.
[9] "17 Milyon Öğrencinin Bilgileri Satıldı", *egitimciyiz.com*, 21 October 2012, available at: http://www.egitimciyiz.com/17-milyon-ogrencinin-bilgileri-satildi.html/
[10] "CHP Milletvekili Atıcı, SGK'nın Veri Paylaşım Kararını Sert Sözlerle Eleştirdi", *turk.internet*.com, 17 January 2013, available at: http://www.turk-internet.com/portal/yazigoster.php?yaziid=40702
[11] "Sağlıkta mahremiyet tartışması başladı", *Radikal*.com, 21 December 2012, available at: http://www.radikal.com.tr/saglik/saglikta_mahremiyet_tartismasi_basladi-1113122

Additionally, Turkey has a mandatory identity card; each card is linked to a unique identity number.[12] The existence of an identity card system enables disparate identifying information about a person that is stored in different databases to be easily linked and analysed through data mining techniques. This creates a significant privacy vulnerability. Plans to introduce a biometric identity card are in progress. Biometrics refers to the measurement of unique and distinctive physical, biological and behavioural characteristics.[13] Particularly in the absence of a strong data protection regime, biometric data – extremely sensitive data – is open to misuse and abuse.

Surveillance of mobile communications

There is a widespread perception in Turkey that mobile communications are monitored by state agencies on a large scale, which, in addition to imperilling the right to privacy, has a chilling effect on freedom of expression.[14]

Turkey has mandatory SIM card registration, with registration tied to the user's national identity number.[15] In the absence of data protection legislation, SIM users' information can be shared with government departments and matched with other private and public databases, enabling the state to create comprehensive profiles of individual citizens. Mandatory SIM card registration facilitates the establishment of extensive databases of user information, eradicating the potential for anonymity of communications, enabling location-tracking, and simplifying communications surveillance and interception.

Internet censorship and surveillance

In February 2014, a controversial new law came into force allowing the Turkish Telecommunications Authority (TIB) to order the removal of content from websites, in some cases without having first obtained a court order. This law amended a 2007 law[16] that introduced internet censorship in Turkey and saw the entirety of the popular website YouTube blocked for a number of months.[17] Data on the

---

[12] Alanur Cavlin Bozbeyoglu "Citizenship rights in a surveillance society: The case of the electronic ID card in Turkey", *Surveillance and Society*, Vol 9, No 1/2 (2011), available at: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/citizenship; see also, Toby Stevens, John Elliott, Anssi Hoikkanen, Ioannis Maghiros, Wainer Lusoli , "The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies", European Commission Joint Research Centre, Institute for Prospective Technological Studies (2010), available at: http://privacygroup.org/wp-content/uploads/2013/09/JRC60959.pdf

[13] "Biometrics: Friend or Foe of Privacy", *Privacy International*, December 2013, available at: https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/biometrics_friend_or_foe.pdf

[14] "Country Reports on Human Rights Practices for 2013: Turkey", United States of America Department of State, Bureau of Democracy, Human Rights and Labor (2013), available at: http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper

[15] "The Mandatory Registration of Prepaid SIM Card Users: White Paper", *GSM Association*, November 2013, available at: http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf. Phones brought into the country from abroad must be registered or they are blocked.

[16] Law No 5651 "on regulation of publications on the internet and combating crimes by means of such publications" entered into force on 23 May 2007.

[17] "Turkey pushes through new raft of 'draconian' internet restrictions", *The Guardian*, 6 February 2014, available at: http://www.theguardian.com/world/2014/feb/06/turkey-internet-

number of websites that have been blocked is not public, but civil society groups estimate that, as of June 2014, more than 44,000 websites are blocked by the TIB.[18]

The new law not only has implications for the right to freedom of expression, but also the right to privacy. Internet service providers were already required to store records of internet activity; the new law extends this requirement to other internet companies. The period of storage is two years.[19] Internet service providers and other companies must provide traffic data (which is insufficiently defined in law), including identifying information, to the TIB on request, without informing users. Once it has obtained the data, the TIB can then retain it indefinitely.[20] Yaman Akdeniz, a law professor at Istanbul's Bilgi University, has referred to the law as an "Orwellian nightmare".[21]

There are private surveillance industry products with invasive capabilities in Turkey. The Citizen Lab, an interdisciplinary laboratory based at the University of Toronto, has found evidence that a programme called "PackageShaper", produced by Blue Coat Systems, a United States-based company, is in Turkey. This programme is used for internet filtering and Citizen Lab has described it as a "dual-use" technology, because its data-gathering capacities could be used for surveillance.[22] Spyware – programmes that give a customer the ability to observe and control a targeted person's computer – produced by Italian company Hacking Team and by United Kingdom-German company Gamma International, has also been found in Turkey.[23] Such spyware permits a customer to intercept passwords and emails as a user of the device types them in and even remotely turn on a device's microphone to record conversations going on nearby.[24]

Expanded powers of National Intelligence Agency

In April 2014, a law expanding the powers of the National Intelligence Agency entered into force.[25] This law has been strongly criticised by human rights groups, with Human Rights Watch stating:[26]

---

law-censorship-democracy-threat-opposition; see also, Catherine Stupp, "Unclear internet law spells uncertain future for free expression in Turkey", *Index on Censorship,* 12 February 2014, available at: http://www.indexoncensorship.org/2014/02/amendments-internet-law-approved-turkish-parliament-remain-murky/

[18] See, http://engelliweb.com/kategoriler/ a site that monitors which sites have been blocked in Turkey.

[19] "Turkey: Gul Should Veto New Internet Rules", *Human Rights Watch,* 6 February 2014, https://www.hrw.org/news/2014/02/06/turkey-gul-should-veto-new-internet-rules

[20] See Stupp above.

[21] "Turkey's new Internet law is the first step toward surveillance society,' says cyberlaw expert", *Hurriyet Daily News*, 24 February 2014, available at: http://www.hurriyetdailynews.com/turkeys-new-internet-law-is-the-first-step-toward-surveillance-society-says-cyberlaw-expert.aspx?pageID=238&nID=62815&NewsCatID=338

[22] Summary Analysis of Blue Coat "Countries of Interest", *Citizen Lab,* 15 January 2013, available at: https://citizenlab.org/2013/01/appendix-a-summary-analysis-of-blue-coat-countries-of-interest/

[23] "Mapping Hacking Team's "Untraceable" Spyware", *Citizen Lab,* 17 February 2014, available at: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

[24] Morgan Marquis-Boire et al, "For Their Eyes Only: the Commercialization of Digital Spying", May 2013, available at: https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf

[25] The "Law Amending the Law on State Intelligence Services and the National Intelligence Agency" (Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik

> The new law gives the intelligence agency sweeping powers to amass private data, documents, and information about individuals in all forms without the need for a court order from public bodies, banks, archives, companies, and other legal entities, as well as from organizations without legal status. The law makes provision of all such information to MİT [the National Intelligence Agency] obligatory and overrides provisions in any other laws or bylaws limiting the provision of such data.
>
> Another provision of the new law makes it a criminal offense punishable with prison sentences ranging from two to five years to prevent the MİT from carrying out its duties and exercising its authority. So failure to supply private data requested by the agency could be interpreted as obstructing the agency from carrying out its work and could be punishable with a prison sentence.
>
> Turkey's laws in general fail to enshrine any clear limitations on the scope of retention and access to private data. The new MİT law fundamentally undermines the right to privacy by permitting the agency unfettered access to data without judicial oversight or review.
>
> Furthermore, the new law permits the agency to "collect data relating to external intelligence, national defense, terrorism, international crimes and cyber security passing via telecommunication channels" without specifying the need for a court order. Beyond this measure, with the authorization of the head of agency or deputy heads, the law gives the intelligence agency the authority to intercept calls overseas, and calls by foreigners and pay phones, and analyze and store the data.

Recommendations

We recommend that the government of Turkey:

- Immediately repeals the April 2014 amendments to Law No 6532 (on State Intelligence Services and National Intelligence Agency);
- Immediately repeals the February 2014 amendments to Law No 5651 (on regulation of publications on the internet and combating crimes by means of such publications);
- As an urgent matter, enacts data protection legislation that complies with international standards and establishes an independent data protection authority;
- Removes the requirement for mandatory SIM card registration;

Yapılmasına Dair Kanunu, no. 6532); see, "Turkish Parliament Gives Spy Agency Controversial New Powers", *Financial Times*, 17 April 2014, available at: http://www.ft.com/cms/s/0/495a79cc-c656-11e3-ba0e-00144feabdc0.html#axzz33r1u66bk

[26] "Turkey: Spy Agency Law Opens Door to Abuse", *Human Rights Watch,* 29 April 2014, available at: http://www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse

- Recognises and takes steps towards compliance with the *International Principles on the Application of Human Rights to Communications Surveillance*;[27]

- Ensures that there are appropriate controls to prevent the use of private surveillance industry products to facilitate human rights abuses.

[27] Available at: https://en.necessaryandproportionate.org/text