

Access Now submission to the United Nations Human Rights Council, on the Universal Periodic Review 2019 Third Cycle for Italy

About Access Now

1. Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Through representation around the world, including in the European Union, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. We engage with an action focused global community, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.
2. Access Now advocates an approach to digital security that promotes user rights, including privacy and freedom of expression. Access Now has worked extensively on digital rights including on free expression and web blocking, regulation of Net Neutrality, and data protection.

Domestic and international human rights obligations

3. This is the third Universal Periodic Review for Italy after having been reviewed in 2010 and 2014.¹ In the 2010 review, the government received 92 recommendations, 80 of which were accepted and 12 rejected.² In the 2014 review, they received 186 recommendations, 176 of which were accepted and 10 noted.³ None of the 2nd Cycle recommendations addressed freedom of expression or the right to privacy.
4. Italy has ratified the International Covenant on Civil and Political Rights ("ICCPR"), and the International Covenant on Economic, Social, and Cultural Rights ("ICESCR").
5. Part I of the Italian Constitutions sets out the duties and rights of citizens, with Article 13 affirming that "no one may be detained, inspected, or searched nor otherwise subjected to any restriction of personal liberty except by order of the Judiciary stating a reason and only in such cases and in such manner as provided by the law."
6. Article 15 of the Italian Constitution states that "freedom and confidentiality of correspondence and of every other form of communication is inviolable." However, it goes on to specify that "limitations may only be imposed by judicial decision stating the reasons and in accordance with the guarantees provided by the law."⁴
7. Article 21 focuses on freedom of expression explicitly, stating "anyone has the right to freely express their thoughts in speech, writing, or any other form of communication." It goes on to explicitly protect the right of the press to be free from authorisation or censorship.

¹ <https://www.upr-info.org/en/review/Italy>.

² https://www.upr-info.org/sites/default/files/document/italy/session_7_-_february_2010/recommendationstoitaly2010.pdf.

³ https://www.upr-info.org/sites/default/files/document/italy/session_20_-_october_2014/recommendations_and_pledges_italy_2014.pdf.

⁴ https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf.

Developments of digital rights in Italy

Privacy and Surveillance

8. In the first half of 2017, Members of the Italian parliament advanced a proposal for regulating government hacking activities, including the use of hacking tools, such as Trojans and other software designed to extract data from internet-connected devices. Access Now submitted feedback regarding the draft law's impact on human rights.⁵ We praised the positive aspects of the law, but also suggested improvements, citing to our 2016 report and recommendations, *A Human Rights Response to Government Hacking*.⁶ The law was not further pursued, and unfortunately when legislation was eventually passed in May 2017 it was narrow and did not provide adequate safeguards for human rights.⁷
9. In August 2017, Access Now learned through a freedom of information request that Italian police forces have power to conduct government hacking as stipulated in the April 2015 Italian Criminal Procedural code Art. 234: "It is always permitted the acquisition of documents and computer data stored abroad, including those not available to the public, with the consent, in this last case, of the legitimate holder."⁸
10. In an earlier inquiry in 2016 into "Encryption of Data Questionnaire" which was circulated to the EU Member States by the Council (this informs the legislative process in the EU institutions), Access Now learned that Italian law enforcement agencies conduct wiretapping of encrypted data by the so-called "trojan inoculation" technique - subject to a judicial order.⁹ From those same documents we learned that the forensic analysis often inadvertently reveals "financial and personal data... also any other kind of information were found in sized encrypted data."
11. The same questionnaire from 2016 revealed that Italian law enforcement works with third parties "industries/companies" in order to try and decrypt the intercepted data.¹⁰
12. In 2015, the government passed an anti-terrorism law which extended the period internet service providers must keep users' metadata, from 12 months to 24 months. The information that must be retained includes broadband internet data, internet telephony, internet use via mobile phone, and email activity.¹¹ This law was passed in spite of the 2014 ruling by the European Court of Justice finding such data retention in violation of human rights.¹²

Freedom of Expression

⁵ <https://www.accessnow.org/cms/assets/uploads/2017/05/Access-Now-Comment-Disciplina-dell'uso-dei-captatori-legali.pdf>

⁶ <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>

⁷ See <https://www.privacyinternational.org/blog/2423/italys-supreme-court-decision-limits-hacking-powers-and-applies-safeguards>.

⁸ https://www.asktheeu.org/en/request/responses_to_the_questionnaire_o#incoming-14200

⁹ <https://www.accessnow.org/eu-ministers-targeting-encryption-need-know/>

¹⁰ See responses to question 6 of the Encryption of Data Questionnaire:

<https://www.asktheeu.org/en/request/3347/response/11727/attach/10/Encryption%20questionnaire%20IT.pdf>

¹¹ <https://freedomhouse.org/report/freedom-net/2016/italy>

¹² <https://edri.org/italy-anti-terrorism-decree-strengthen-government-surveillance/>.

13. Although Italy considered reformatioes to its defamation laws in 2014, defamation remains a criminal offense, leaving the press particularly vulnerable to suits because defamation committed by medium of the press is an enhanced offense.^{13 14}
14. In an effort to combat online disinformation and fake news, in 2018, leading up to the March elections, the former interior minister announced an initiative allowing citizens to report fake news to the postal police, the division of the Italy state police charged with investigating cybercrime.¹⁵

Connectivity

15. In 2017, Italy ranked 47th on the International Telecommunications Union's Information and Communications Technology Development Index, one place down from its 2016 ranking.¹⁶ About 70% of households have internet access, lagging behind the 82.5% average for Europe.¹⁷
16. Regarding internet use, 61.32% of individuals in Italy use the internet, compared to the 77.9% average for Europe.¹⁸

Violations of freedom of expression

16. Italy was ranked 46 out of 180 countries in the World Press Freedom Index of 2018 by Reporters Without Borders (RSF). The Index reported that while journalists generally enjoy a lot of protection from the police that, "many journalists are also worried by the recent election victory of the Five Star Movement (M5S), which is often vocal in its criticism of the media and does not hesitate to name the journalists it doesn't like. Journalists increasingly opt to censor themselves because of the pressure from politicians. Under a proposed new law, defaming politicians, judges or civil servants would be punishable by six to nine years in prison."¹⁹
17. In 2018 there were several controversies where the grounds for police searches came into question. In the case of Salvo Palazzolo, a reporter who specializes in covering the Sicilian mafia and other criminal records, RSF argues that the police search and seizures of his property "violated the confidentiality of his sources."²⁰

Violations of the right to privacy

18. Over the past several years, Italy has gained a reputation as a safe haven for cyber surveillance companies which carry out their international operations from their jurisdiction. After leaked documents showed that private surveillance technology company HackingTeam was engaged in selling spyware to repressive regimes, aiding in the

¹³ <https://www.coe.int/en/web/commissioner/-/defamation-in-italy-a-draft-law-to-be-changed>.

¹⁴ <https://www.altalex.com/documents/news/2014/10/28/dei-delitti-contro-la-persona>.

¹⁵ <https://www.refworld.org/docid/5be16b0f13.html>.

¹⁶ <https://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economytab&ITA>.

¹⁷ Id.

¹⁸ Id.

¹⁹ <https://rsf.org/en/italy>

²⁰ <https://rsf.org/en/news/italy-police-search-violates-confidentiality-anti-mafia-reporters-sources>

compromise and surveillance of human rights activists, journalists and other civil society actors, the Italian authorities raided the premises of the company and revoked the relevant export licenses they had been granted.²¹

19. A similar case unfolded when a spyware company known as Area (referred to as Area Spa by some media) was found out to be in breach of Italy's export rules. The authorities also acted quickly in the first instance and raided the offices, but the official investigation never came to a conclusion, and as far as we are aware, the company is still operational with those licenses.^{22/23}
20. In March 2016, the UN Human Rights Committee raised surveillance technology exports as an area of concern for Italy's compliance with its international obligations. During the review of Italy's obligations under the International Covenant on Civil and Political Rights (ICCPR), the Human Rights Committee expressed its concerns about "allegations that companies in the State of the investigation provided online surveillance equipment to foreign governments who have committed serious violations of human rights," and recommended that the Italian authorities "take measures to ensure that all companies within their jurisdiction, in particular those producing technology, respect human rights standards in their activities abroad."²⁴

Recommendations

21. Government hacking and surveillance pose grave risks to human rights, particularly to the rights of freedom of expression and privacy. Therefore, we recommend that:
 - a. Italy must adhere to the 13 International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles")²⁵ to protect human rights. These principles lead to certain safeguards described in our guidance on government hacking, which the Italian government must implement including mechanisms for transparency, robust oversight, and access to remedy;²⁶
 - b. Italy must end its hacking for surveillance purposes until and unless they can be demonstrated to be in full compliance with applicable international human rights law, including the 13 Necessary and proportionate Principles; and
 - c. Italy must decriminalize defamation. The criminalization of defamation has particularly stifled freedom of expression among the media, as evidenced by the

²¹ https://motherboard.vice.com/en_us/article/78k8dq/hacking-team-has-lost-its-license-to-export-spyware

²² News report on Area Spa context: https://motherboard.vice.com/en_us/article/gv5knx/italian-cops-raid-surveillance-tech-company-area-spa-selling-spy-gear-to-syria

²³ Access Now partnered with other NGOs in order to ask the Italian authorities to investigate the matter, but no follow-up was ever issued to our knowledge. <https://www.accessnow.org/italy-revoke-export-license-cyber-surveillance-company/>

²⁴

http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fITA%2fCO%2f6&Lang=en

²⁵ <https://necessaryandproportionate.org/principles>

²⁶ <https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf>

number of journalists targeted through legal actions.²⁷ By removing prison sentences and excessive fines for defamation, Italy would strengthen free expression.

22. Italy must make stronger efforts to ensure that companies within its jurisdiction do not export surveillance technology to countries with a record of serious human rights violations. To that end, we recommend that:
 - a. the government must more closely scrutinize corporate dealings with foreign governments in the technology sector, including by requiring human rights due diligence regarding supply chains, end-users, and intended and potential uses of technology exports;
 - b. Italy must make its export licensing process more accountable to human rights, by considering the human rights record of the importing country, and the human rights due diligence of the exporting company, in the licensing process;
 - c. and Italy must increase transparency of its export licensing, by disclosing applications and determinations and investigating cases of potential misuse.
23. The UPR is an important U.N. process aimed at addressing human rights issues all across the globe. It is a rare mechanism through which citizens around the world get to work with governments to improve human rights and hold them accountable to international law. Access Now is grateful to make this submission.
24. For additional information, please contact Access Now staff Peter Micek (peter@accessnow.org).

²⁷ <https://www.rcmediafreedom.eu/Tools/Legal-Resources/Legal-Defence-Centres-Fighting-for-Press-Freedom-in-Italy>.