Access Now Submission to the United Nations Human Rights Council on the Universal Periodic Review 2020 Third Cycle for the United States

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 in 14 countries around the world, including engagement with stakeholders and policymakers in North America, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet 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 robust security policies that protect 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.

Introduction

3. The Universal Periodic Review (UPR) is an important U.N. aimed at addressing human rights issues across the globe. Access Now welcomes this opportunity to contribute to the United States' third review cycle. This submission examines freedom of expression and the right to privacy as it relates to the digital age.
4. This is the third review for the United States, last reviewed in May 2015. The US government received 343 recommendations during the UPR in Geneva, of which 150 were accepted and 193 others noted.

International and domestic human rights obligations

5. The United States has signed onto various international human rights instruments, including the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, the International Convention on the Elimination of All Forms of Racial Discrimination, and the Convention on the Elimination of all Forms of Discrimination Against Women.

6. The first amendment to the U.S. Constitution establishes a fundamental right to freedom of speech and freedom of the press. The fourteenth amendment to the U.S. Constitution establishes the right to equality, life, and liberty.

Deterioration of U.S. global commitment to human rights

7. In June 2018 the United States pulled out of the United Nations Human Rights Council (HRC). This action leaves doubt as to what, if any, commitment the United States maintains toward human rights, internet freedom, and the rule of law online. This withdrawal gives rise to many uncertainties such as what international mechanisms the United States will engage in to respond to human rights violations around the world and how the U.S. will protect NGOs and activists who bring complaints and evidence to the HRC.

Data protection, privacy, and cybersecurity

8. On February 27, 2019 the U.S. Senate Committee on Commerce, Science, and Transportation convened a public hearing to discuss "Policy Principles for a Federal Data Privacy Framework in the United States."[1] However, five of the six witnesses invited to testify represented the ICT industry itself, companies whose profit models depend in varying degrees on limiting restrictions to their use of personal data. Internet users whose data passes through the United States currently have very little legal protection when it comes to understanding and controlling how their personal information is stored, utilized, and shared by private companies.[2]

9. Absent federal action, states have been taking the initiative to better protect individuals' human rights in the digital age. Since 2018, all 50 states have implemented a data breach notification law, enabling people in every state to acquire information that is useful for mitigating the impact of a devastating data breach.

10. The California Consumer Privacy Act, which will take effect in January 2020, is a benchmark state data privacy law that provides California residents the ability to opt-out of a company's sale of their personal information and to request deletion of personal information (with certain exceptions).[3]

11. Vermont passed a "data broker" law in 2018 which requires data brokers — those who profit from gathering and selling our data — to register with the state and prohibits them from acquiring our personal information in a fraudulent way.[4]

12. States, such as New York, Colorado, and Vermont, have laws requiring financial service companies to take steps to protect confidential information.[5]

---

[1] Policy Principles for a Federal Data Privacy Framework in the United States, U.S. Senate Committee on Commerce, Science, and Transportation, 2019
[2] U.S. Senate excludes civil society from critical data protection hearing, Access Now, 2019
[3] SB-1121 California Consumer Privacy Act of 2018, California Legislative Information, 2018
[4] Data brokers are selling your secrets. How states are trying to stop them, The Washington Post, 2019
[5] Colorado and Vermont Adopt Cybersecurity Rules Covering Broker-Dealers and Investment Advisers, Proskauer, 2017

13. Washington, Hawaii, and Rhode Island have previously introduced bills seeking to improve state cybersecurity practices, such as by establishing an agency dedicated to cybersecurity issues.[6]

14. California recently passed a law that requires manufacturers of "Internet of Things" devices — such as smart watches, speakers, and refrigerators — to equip our devices with reasonable security features.[7]

Freedom of expression

15. Citing free speech concerns, the United States chose not to join several other countries and companies in adopting the Christchurch Call on May 15, 2019, following the terrorist attacks in Christchurch, New Zealand, of which video footage was streamed over social media sites.[8] This decision is consistent with the longstanding position of the U.S. government to not call on itself nor on other countries to take action that is inconsistent with U.S. First Amendment free speech principles. In a similar move made in 2016, the U.S. was relatively isolated in voting against a (not legally binding) U.N. General Assembly resolution about condemning the glorification of Nazism.[9]

Surveillance

16. Certain surveillance laws and provisions in the United States, including Section 215 of the Patriot Act, which have provided the basis for U.S. intelligence agencies conducting indiscriminate surveillance on a massive scale, impacting millions of people around the world, are set to expire on December 15, 2019. It is crucial that congressional leadership facilitate an open and in-depth public debate over the power and reach of the U.S. surveillance apparatus.[10]

17. The NSA announced in June 2018 that it had deleted its entire database of call detail records due to "technical irregularities." Such "irregularities" resulted in the agency receiving data it was not authorized to collect.[11]

18. Seattle and several cities in California, such as Oakland and Berkeley, have passed "Community Control Over Police Surveillance" (CCOPS) laws that enable community oversight of local police departments' acquisition of new surveillance technologies.[12]

---

[6] Cybersecurity Legislation 2018, National Conference of State Legislators, 2018
[7] What you need to know about California's IoT security legislation, GCN, 2018
[8] Statement on Christchurch Call for Action, U.S. Embassy & Consulate in New Zealand, 2019
[9] Why the Christchurch Call to Remove Online Terror Content Triggers Free Speech Concerns, Just Security, 2019
[10] Privacy advocates call on U.S. Congress to release information crucial for surveillance reform debate, Access Now, 2019
[11] NSA Reports Data Deletion, National Security Agency, 2018
[12] How Cities Are Reining in Out-of-Control Policing Tech, Slate, 2018

19. San Francisco and Oakland, California and Somerville, Massachusetts banned facial recognition technology, among other cities.[13]

Recommendations

The United States should improve its human rights record and treatment of digital rights in several areas. We accordingly recommend that the government of the United States:

20. Rejoin the United Nations Human Rights Council;

21. The U.S. Senate and House Judiciary Committees' leaders should release critical information regarding the current implementation of U.S. surveillance laws;

22. Implement a comprehensive data privacy and protection framework that would guarantee fundamental privacy rights and control over one's personal information for everyone whose data passes through the United States, whether it be through a government agency or private company;

23. Meaningfully include consumer, civil, and digital rights organizations representing individuals in any federal data privacy debate;

24. Create a grant program for companies investing in privacy-protective business models and practices, including any model not based around exploiting user data;

25. Commit to the protection of digital security, including encryption, and investment in research and development to explore the best methods for protecting user data;

26. Create a board to develop security best practices for Internet of Things devices (Congressman Ted Lieu [D-CA-33] and other members of Congress have already introduced a bill that would take this approach);

27. Invest in companies that explore and develop systems for greater interoperability of edge providers;

28. Sign and ratify all major international treaties and covenants on the protection and promotion of human, environmental, and labor rights;

29. Research the harms of data breaches of non-financial personal data and potential redress mechanisms to respond to those harms;

[13] Beyond San Francisco, more countries are saying no to facial recognition, CNN, 2019

30. Establish an independent data protection commission with authority and resources to monitor implementation, conduct investigations, and sanction entities in the event of data protection violations.

31. 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 are afforded the opportunity to work with governments to improve human rights and hold them accountable to international law. Access Now is grateful to submit this review.

32. For additional information, please contact Access Now General Counsel Peter Micek (peter@accessnow.org).