Access Now submission to the United Nations Human Rights Council, on the Universal Periodic Review 2018 Cycle – Germany

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 10 countries around the world, including engagement with stakeholders and policymakers in Germany, 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 good security policies that protect user rights, including privacy and freedom of expression. Access Now has worked extensively to draw attention to digital rights issues in Germany, including encryption and mass surveillance.

Role of German human rights assessment

3. This is the third review for Germany, last reviewed in April 2013 where the German government received 203 recommendations in the area of human rights at the Universal Periodic Review mechanism (UPR) in Geneva.
4. In January 2018, Germany will take over the chairmanship of the Freedom Online Coalition (FOC); an international coalition of 30 governments which work closely together to coordinate their diplomatic efforts and engage with civil society and the private sector to support Internet freedom – free expression, association, assembly, and privacy online – worldwide. Germany's commitments to protect and promote human rights in the digital era are exceptionally important given their increasing leadership in fora such as the FOC and the Global Forum on Cyber Expertise (GFCE), through which they impact policy around the globe. In addition, as the current G20 host country (or President), Germany, has put digitalisation and the digital economy at the heart of the G20 agenda for the first time.

Domestic and international human rights obligations

5. Germany has signed onto various international human rights instruments, including the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). Article 17 of the ICCPR and Article 8 of the ECHR ensure the right to privacy and Article 19 of the ICCPR and Article 10 of the ECHR guarantee the right to freedom of expression and freedom of opinion. As a European Union member state, the Charter of Fundamental Rights of the European Union (Charter) is applicable to Germany. Article 7 and 8 of the Charter enshrines the fundamental rights to privacy and data protection.

6. The Basic Law for the Federal Republic of Germany also provides for judicially enforceable rights to privacy and free expression.[1] Article 5 guarantees individuals' right to express and disseminate their opinions and prohibits censorship. Article 10 guarantees the inviolability of the privacy of correspondence, posts and telecommunications.
7. International human rights entities have consistently affirmed these rights extend to online expression and communication. In December 2013, the United Nations General Assembly adopted Resolution 68/167, which expressed concern at the human rights violations caused by surveillance and interception of communications, and affirmed that the rights held by people offline must also be protected online, and called upon all States to respect the right to privacy in digital communication. In May 2015, UN Special Rapporteur on freedom of expression David Kaye released a report which asserted the essential role of encryption and anonymity in the ensuring the rights to freedom of expression and privacy on the internet. Encryption and anonymity are deserving of "strong protection" because they "enable individuals to exercise their rights to freedom of opinion and expression in the digital age," the Special Rapporteur found.
8. In the past few years Germany has positioned itself at the forefront of the privacy debate internationally, asserting the need to protect privacy and condemning government surveillance. Notably, Germany joined Brazil in promoting the UN resolution on the right to privacy in the digital age, which led to the creation of the Special Rapporteur on the right to privacy.

Violations of free expression

9. In June 2017, German lawmakers passed the Social Network Enforcement Act ("NetzDG") which enables the government to issue a fine of up to €50 million to social media platforms that fail to take down content labelled as hate speech, fake news or extremist. Digital rights and free speech activists have opposed the law, arguing that it places too large of a burden on social media companies rather than law enforcement.[2] Moreover, the financial penalty encourages companies to take an overbroad implementation and restricting legal but controversial speech in order to avoid fines[3]. To address the law, UN Special Rapporteur on freedom of expression David Kaye wrote to the High Commissioner for Human Rights emphasizing that "many of the violations covered by the bill are highly dependent on context, context which platforms are in no position to assess."[4] He added that "the obligations placed upon private companies to regulate and take down content raises concern with respect to freedom of expression". Countering illegal hate speech online is an important issue and requires open and

[1] See Basic Law at https://www.btg-bestellservice.de/pdf/80201000.pdf.
[2] Coalition letter, Germany's Draft Network Enforcement Law is a threat to freedom of expression, established EU law and the goals of the Commission's DSM Strategy - the Commission must take action, 22 May 2017, https://edri.org/files/201705-letter-germany-network-enforcement-law.pdf.
[3] Janet Burns, 'Germany to Social Media Sites: Remove Hate Speech in 24 Hours Or $57 Million Fines' (Forbes, 30 June 2017) <https://www.forbes.com/sites/janetwburns/2017/06/30/germany-now-allows-up-to-57m-in-fines-if-facebook-doesnt-remove-hate-speech-fast/#6246df77761d>
[4] David Kaye's letter (1 June 2017), http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf

transparent discussions to ensure compliance with human rights obligations.[5]

Surveillance and whistleblowing

10. In 2014, leaked confidential documents revealed that the Bundesnachrichtendienst (BND) requested an additional 300 million Euros from the German Parliament to disproportionately expand its surveillance program in an effort to rival those of the United States and the United Kingdom. The program was intended to overhaul the BND's digital infrastructure and enhance Germany's surveillance and metadata collection capability. It was planned to introduce real-time monitoring of social media sites.[6] The leaked documents also revealed that Bundeswehr-Universität München, a German military research university, was conducting a study on "automated monitoring of internet content" of social media.[7]
11. The German Federal Public Prosecutor opened a criminal investigation for treason against journalists Markus Beckedahl, Andre Meister, and an unknown source in August 2015.[8] The journalists had published documents regarding Germany's plans for launching bulk surveillance programs on their Netzpolitik blog, one of the most influential online platforms for digital freedom in Germany. Following widespread protests the investigation was put on hold. The mere fact of the treason investigation, however, and forcing journalists to reveal the identity of their sources, have chilling effects on media freedom by dissuading whistleblowers from speaking out, and reporters from publishing their stories.[9] In addition, the German foreign intelligence agency reportedly surveilled foreign journalists.[10]
12. Germany must ensure robust protection and promotion of access to information, and take caution to ensure that it does not chill expression or obstruct journalism through its prosecutory arms. The country must remember its own commitment to privacy and whistleblower protection, which the govenrment has trumpeted so many times on the international stage, including at UN level. Governments have a duty to uphold fundamental rights outside and within their borders at all times, not just when it is politically convenient to do so.

---

[5] A digital rights approach to proposals for preventing or countering violent extremism online (Access Now, November 2016), https://www.accessnow.org/cms/assets/uploads/2016/10/CVE-online-10.27.pdf.
[6] John Goetz, Hans Leyendecker and Frederik Obermaier, "BND will soziale Netzwerke live ausforschen" (Süddeutsche Zeitung, 31 May 2014) <http://www.sueddeutsche.de/digital/auslandsgeheimdienst-bnd-will-soziale-netzwerke-live-ausforschen-1.1979677>
[7] Alexander Plaum, 'Looking at NSA & GCHQ as role models: German intelligence plans their own mass spying program' (Access Now, 4 June 2014) <https://www.accessnow.org/nsa-gchq-as-role-models-german-intelligence-plans-their-own-mass-spying/>
[8] Cyrus Farivar, "After publishing secret spy docs, German news site investigated for treason" ' (Ars Technica, 30 July 2015) <https://arstechnica.com/tech-policy/2015/07/after-publishing-secret-spy-docs-german-news-site-investigated-for-treason/>
[9] Estelle Massé, 'Netzpolitik.org reports on government surveillance, is investigated for treason' (Access Now, 3 August 2015) <https://www.accessnow.org/netzpolitikorg-reports-on-government-surveillance-is-investigated-for-trea/>
[10] Reporters Without Borders Germany, German intelligence agency violates freedom of the press (EDRi 8 March 2017)
https://edri.org/german-intelligence-agency-violates-freedom-of-the-press/

Undermining encryption

13. Germany has voiced its support for "more and better encryption" and in its Digital Agenda, the German government resolved to become the "world leader in encryption[11]. However, members of its government have vocally opposed encryption and it has enacted anti-encryption policy. In August 2016, German Minister of Interior Thomas de Maiziere met with French Minister of Interior Bernard Cazeneuve to discuss "security demands" for Europe, which included "arming [European] democracies against the question of encryption."[12] In response to this statement, together with a push from justice ministers in the EU, the European Commission has launched an inquiry into law enforcement access to e-evidence; as a part of which they are looking for "solutions" to issues such as encryption, faced by law enforcement. In June 2017 the German Parliament passed a bill allowing the government to hack into encrypted messaging services during certain criminal investigations. Previously, German police could tap into a suspect's SMS communications and phone conversations if the alleged crime was sufficiently severe. However, they were prohibited from viewing messages sent through end-to-end encryption services, such as WhatsApp, Signal and Threema. The new legislation permits use of spyware to infiltrate a suspect's device and read messages before they are encrypted, allowing remote searches on a suspect's device in specific cases.[13]

Trade of spyware

14. In August 2012, security researchers turned up a FinSpy server in Ethiopia. FinSpy is a remote monitoring tool which is installed onto a targeted device via an external malware link; the tool can then capture the target's every online move and keystroke. It was developed and sold by the UK-German firm Gamma International, and subsequently traded through an independent Munich-based company operating under the name of FinFisher. In 2014 there was a German parliamentary inquiry into the sale of surveillance technologies to foreign governments and in response the German government stated that over the past decade, it provided German companies with licenses to export surveillance technologies to at least 25 countries, many of which have long history of human rights abuse. The inquiry revealed that between 2003 and 2013, surveillance technologies were exported to Albania, Argentina, Chile, India, Indonesia, Qatar, Kosovo, Kuwait, Lebanon, Malaysia, Morocco, Mexico, Norway, Oman, Pakistan, Russia, Saudi Arabia, Switzerland, Singapore, Taiwan, Turkey, Turkmenistan, USA and

---

[11] Thorsten Benner and Mirko Hohmann 'How Europe Can Get Encryption Right' (Politico 13 April 2017) <http://www.politico.eu/article/how-europe-can-get-encryption-right-data-protection-privacy-counter-terrorism-technology/>

[12] Lucie Krahulcova, 'Encryption under heavy fire as Franco-German ministerial duo makes demands' (Access Now, 23 August 2016) <https://www.accessnow.org/encryption-heavy-fire-franco-german-ministerial-duo-makes-demands/>

[13] Victor Brechenmacher, 'German government to spy on encrypted messaging services' (Politico, 22 June 2017) <http://www.politico.eu/article/german-government-to-spy-on-encrypted-messaging-services/>

the UAE.[14]

Introducing data retention

15. In spite of the data retention ruling of the Court of Justice of the European Union at the end of 2015 finding data retention to interfere with fundamental rights, Germany passed a new law reintroducing data retention. The law introduces a new section to the German Telecommunications Act and is very similar to the former law on data retention from 2008 which was struck down by the Federal Constitutional Court in 2010.[15]
16. In 2017, a transparency report released by Telefonica, one of the world's largest telcos, revealed details about requests from law enforcement to produce stored and real-time user data, to block or filter internet content, and to shut down network services. The data provided by Telefonica indicates that requests for "historical user data" have increased, including in Germany which made 172,033 requests for such data in 2015. Historical user data requests allow a government to receive information on the name and address of user, the data to identify the source and destination of a specific communication; the date, time and duration of the communication; the type of communication; the identity of the communication equipment; and the location of the user or device[16].

Setback for data protection

17. Germany has historically been a leader in the protection of personal data. The country's commitment to data protection was however challenged during the negotiations of the EU General Data Protection Regulation (GDPR) when the German Interior Ministry sought to slow down the discussions.[17] Similarly, when implementing the GDPR, the German Federal government introduced provisions in their draft law which deviated from the GDPR that could cause legal uncertainty and market fragmentation in the EU.[18] For instance, the government suggested provisions that would have limited users' rights to be informed, and to control how and why a company processes their information. This proposal not only failed to pass muster from a fundamental rights perspective but was also in clear violation of the GDPR.[19] The German implementation bill was then

[14] Brugger, Agnieszka, "Kleine Anfrage zu Spähsoftware" (blog, 2014) <http://www.agnieszka-brugger.de/hauptmenue/nachrichten/nachricht/datum/2014/08/25/kleine-anfrage-zu-spaehsoftware/>
[15] Privacy International, "National Data Retention Laws since the CJEU's Tele-2/Watson judgment" (September 2017), https://privacyinternational.org/sites/default/files/Data%20Retention_2017.pdf.
[16] Peter Micek and Alyse Rankin, "Telefonica opens up as transparency standards improve" (Access Now, 19 January 2017) <https://www.accessnow.org/telefonica-opens-transparency-standards-improve/>
[17] Claus Hecking, "EU Council: German officials are slowing down European data protection rules" (Der Spiegel, 2 December 2013) <http://www.spiegel.de/netzwelt/netzpolitik/deutsche-beamte-bremsen-europas-datenschutz-aus-a-936704.html>
[18] Ingo Dachwitz, "Methode de Maizière: Wer viel Datenschutzabbau fordert, bekommt am Ende immer noch genug" (Netzpolitk, 28 April 2017) <https://netzpolitik.org/2017/methode-de-maiziere-wer-viel-datenschutzabbau-fordert-bekommt-am-ende-immer-noch-genug/>
[19] David Meyer, "Critics: Germany's GDPR implementation riddled with holes, illegalities" (IAPP, 15 December 2016) <https://iapp.org/news/a/critics-germanys-gdpr-implementation-riddled-with-holes-illegalities/>

improved before adoption and many concluded that “the worst had been avoided” but the end result remains underwhelming for the furthering of users rights.[20]

Recommendations

Access Now recommends that Germany continue its advocacy in support of the development of international standards on the human right to privacy, while also taking these steps:

1. Match international commitments with national laws and policies that fully respect human rights standards, including the Charter of Fundamental Rights, through:
    a. Human rights respecting implementation of the General Data Protection Regulation (GDPR);
    b. Limitations on and safeguards to prevent unlawful surveillance; and
    c. Elimination of data retention requirements.
2. Support the EU-level reform on the confidentiality of communications and online tracking (ePrivacy reform).
3. Respect human rights principles in law enforcement including through a presumptive prohibition on government hacking, proactive and explicit support for access to strong enryption without hindrance, and continued vigilance against data retention requirements.
4. Support the EU and its member states in identifying, strengthening, and implementing human rights safeguards through export controls on surveillance technology.

[20] Estelle Masse, “Only a year until the GDPR becomes applicable: Is Europe ready? (Access Now, 14 June 2017) <https://www.accessnow.org/year-gdpr-becomes-applicable-europe-ready/>