The right to privacy in the digital age

APRIL 2018

UN HUMAN RIGHTS COUNCIL ADOPTED RESOLUTION 34/7

Authors: INCLO. American Civil Liberties Union (ACLU, United States), Association for Civil Rights in Israel (ACRI), Canadian Civil Liberties Association (CCLA), Centro de Estudios Legales y Sociales (CELS, Argentina), Dejusticia (Colombia), Egyptian Initiative for Personal Rights (EIPR), Human Rights Law Network (HRLN, India), Hungarian Civil Liberties Union (HCLU), International Human Rights Group Agora (Russia), Irish Council for Civil Liberties (ICCL), Kenya Human Rights Commission (KHRC), Legal Resources Centre (LRC, South Africa), Liberty (United Kingdom).

The right to privacy in the digital age

Introduction

The International Network of Civil Liberties Organizations (INCLO) would like to thank the Office of the High Commissioner for Human Rights for the opportunity to provide input on human rights challenges relating to privacy in the digital age.

In this submission, we briefly set out the issues and challenges facing encryption and anonymity (question no. 3), reliance on data-driven technology (question no. 4), privacy challenges for vulnerable populations (question no. 5) and surveillance and digital communications interceptions (question no. 6).

By addressing these human rights challenges, we reiterate our recommendation that the Human Rights Committee issue a new General Comment on the right to privacy under Article 17 of the International Covenant on Civil and Political Rights (ICCPR). As the right to digital privacy has taken on enormous new significance since the Committee published General Comment 16 in 1988, this revision is urgently required to provide guidance on state obligations under the ICCPR.

I. Encryption and anonymity

Encryption and anonymous speech online are central to our right to privacy and to freedom of expression. These rights are enshrined in international human rights law[1] and are recognized as deserving of strong protections through encryption protocols.[2] Challenges raised by encryption and anonymity rights include:

RESTRICTED ENCRYPTION ACCESS FOR VULNERABLE POPULATIONS AND THE PRESS

Vulnerable populations are particularly affected by access to and availability of encrypted technologies. This is especially true in regions where the rule of law is tenuous and the human rights of specific demographics and minority populations are threatened.[3] Anonymous communications afforded by encryption technologies provide advantages to populations who are discriminated against by providing them safe

---

1 See Article 17 and Article 19 of UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol 999.
2 See UN Human Rights Council, Report of the Special Rapporteur on the Promotion and protection of the Right to Freedom of Opinion and Expression: Report to the Human Rights Council, David Kaye A/HRC/29/32 (22 May 2016) who at p.1 wrote ‘‘encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection.”
3 See Egypt, where LGBTQ communities are under increasing attack from the government and law enforcement agencies. In the fall of 2017, a bill signed by 67 members of parliament threatened to explicitly criminalize same-sex sexual activity. This followed the apparent arrest of audience members at a concert where people waived rainbow flags; Jo Schietti, “Egypt’s ‘Morality police’ get Grinder to trap LGBT community ahead of new homophobic law”, The New Arab, 27 November 2017. Available from https://www.alaraby.co.uk/english/indepth/2017/11/27/egypts-morality-police-get-on-grindr.

forums to congregate, organize, mobilize, and build community.[4] Currently, these encrypted safeguards tend to be under attack in certain states which attempt to either block access to or intercept encryption protocols.[5]

A further challenge is the lack of encryption and anonymity rights for the press and their sources. Despite recognition that freedom of the press is a cornerstone of democratic society,[6] governments and intelligence agencies have attempted to encroach upon this right.[7] A lack of respect for anonymous communications rights assists government justification for accessing the content and communications data of journalists in order to reveal journalists' sources.[8]

RESTRICTIONS OR THREATS TO PRIVATE ENCRYPTION SERVICE PROVIDERS

Private entities are increasingly promoting online anonymity by implementing encryption protocols and developing encrypted communications apps. While this creates a competitive market advantage as people seek out best methods for private communications, this sector is also facing challenges from various states. Intelligence agencies in particular are attempting to force private organisations to either provide tools for encryption or open backdoors in specific circumstances,[9] or to hand over encryption keys,[10] sometimes through naive misunderstandings of how encryption

---

[4] The Egyptian LGBTQ community increasingly relies on encrypted communications like Signal; ibid. https://www.alaraby.co.uk/english/indepth/2017/11/27/egypts-morality-police-get-on-grindr.

[5] See the Egyptian government's blocking of encrypted apps like Signal; Jessica Conditt, "Encrypted Chat App Signal Circumvents Government Censorship", *Engadget,* 21 December 2016. Available from https://www.engadget.com/2016/12/21/signal-egypt-uae-censorship-block-domain-fronting/.

[6] See Goodwin v. the United Kingdom 22 EHRR 123, 27 March 1996 at para 39 "Protection of journalistic sources is one of the basic conditions for press freedom, ... without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest."

[7] See Elizabeth Farries, "Ireland Not Immune to the Threat of Surveillance Against Journalists" *The Journal,* 9 November 2017. Available from http://www.thejournal.ie/author/elizabeth-farries/5547/.

[8] In Ireland, for example the Data Retention and Communications Act 2011 permits access to journalist communications data in contravention of EU law. Available from https://www.iccl.ie/wp-content/uploads/2017/12/DRI-ICCL-DR-submission-13.11.17_Website_EF-edit.pdf.

[9] In the United States, the FBI attempted to force Apple to open an encrypted back door into a smart phone. See Eric Lichtblau and Katie Benner, "Apple Fights Order to unlock San Bernardino Gunman's iPhone", *The New York Times,* 17 February 2016. Available from https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?rref=collection%2Fnewseventcollection%2Fapple-fbi-case&action=click&contentCollection=technology&region=stream&module=stream_unit&version=latest&contentPlacement=4&pgtype=collection.

[10] In Russia, two prominent journalists attempted to sue the federal security agency without success because the agency has attempted to force encrypted messenger apps to hand over encryption keys, which would directly compromise journalist source confidentiality. See Anon.,"Journalists are Challenging Russia's 'anti-terrorist' Demands on Instant Messengers', *Meduza,* 25 October 2017. Available from https://meduza.io/en/news/2017/10/25/journalists-are-challenging-russia-s-anti-terrorist-demands-on-instant-messengers.

actually works.[11] Encrypted applications are also either blocked or at risk of being blocked in certain countries.[12]

ENCRYPTION NEEDS OF THE STATE

States institutions and officials, rather than attempting to curtail encryption, could set a leading example by understanding, endorsing, and adopting strong encryption protocols themselves. The illicit acquisition of top state official emails[13] and government agencies housing the personal information of citizens[14] demonstrates this need. Rote arguments that encryption rights should be restricted due to the threat of use by terrorists, criminal activity, or foreign intelligence agencies do not follow as it is precisely these elements that governments and citizens should be protecting themselves against.[15]

ADDRESSING THESE CHALLENGES

While the rights to privacy and to freedom of expression and opinion are not absolute, they must be rigorously safeguarded. The protective measures applied to private offline communications must also be endorsed in online and digital spaces. Encryption is therefore an ideal technological approach to protecting anonymous communications. Avenues of endorsement might include:

- Educating government, law enforcement, and intelligence agency members on the meaning and mechanisms of encryption, and the support these protocols provide to our fundamental rights;
- Supporting and collaborating with open sourced technologies that provide strong encryption protocols for vulnerable populations; and

---

[11] 83 organisations and experts expressed in a joint statement to the 5 Eyes Alliance that "Attempts to engineer 'backdoors' or other deliberate weaknesses into commercially available encryption software, to require that companies preserve the ability to decrypt user data, or to force service providers to design communications tools in ways that allow government interception are both short sighted and counterproductive". Available from Canadian Civil liberties Association, "83 Organisations and Experts from 5 Nations Demand "Five Eyes" Respect Strong Encryption," 30 June 2017. Available from https://ccla.org/83-organizations-experts-5-nations-demand-five-eyes-respect-strong-encryption/.

[12] Telegram has refused to hand over encryption keys to the Federal Security Service and authorities now have a formal ground to block the app in Russia. See, Tom Spring, "Telegram ordered to hand over encryption keys to Russian authorities", *Threat Post,* 20 March 2018. Available from https://threatpost.com/telegram-ordered-to-hand-over-encryption-keys-to-russian-authorities/130581/.
The Telecom regulator in Russia has successfully applied to the court for the permission to block Telegram. An order was delivered 13 April 2018 with immediate implementation. In Egypt, the open sourced app Signal has out maneuvered the Egyptian government's attempts to block it. See Jessica Conditt, "Encrypted chat app Signal circumvents governmental censorship", *Engadget,* 21 December 2016. Available from https://www.engadget.com/2016/12/21/signal-egypt-uae-censorship-block-domain-fronting/.sinead.

[13] See for example the acquisition of emails belonging to Hillary Clinton and Theresa May.

[14] See for example the global ransomware attack that crippled the NHS and the hack of India's Aadhaar database.

[15] We support the 2016 conclusions of the Netherlands' government report that "it is not appropriate to adopt restrictive legal measures against the development, availability and use of encryption." Brief Van De Ministers Van Veiligheid En Justitie En Van Economische Zaken, 4 January 2016. Available from https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015.

- Providing legal support to companies under government attack through litigation and amicus support.

II. Reliance on data driven technology

HOW NEW TECHNOLOGIES HELP PROMOTE AND PROTECT THE RIGHT TO PRIVACY

Privacy by design and default should be a central element for developing new technologies. The Cambridge Analytica scandal shows how damaging technologies can be to privacy when the design is focused merely on profit or usability.[16] Identifying potential privacy implications before and during the development process is the best way for new technology to help protect privacy. For example, when a smart grid is implemented, it is designed to harvest end users' electricity usage data; however, this can reveal sensitive, private information such as when an end user is home. Therefore, identifying this risk upfront and designing the technology around it can greatly bolster the protection of the right to privacy in the final product.[17]

While building privacy into new technologies is a comprehensive solution, interim technological solutions can also assist people who are reliant on privacy invasive programs and infrastructures. These range from user friendly encryption tools to "smart data agents" to using Artificial Intelligence technology to allow individuals to control their own set of personal data.[18] Private sector actors are key players, and strategies to encourage them to give due consideration for privacy should be explored, potentially including the development of guidelines setting out ethical technology development standards.

THE MAIN CHALLENGES REGARDING THE IMPACT ON THE RIGHT TO PRIVACY AND OTHER HUMAN RIGHTS

The proliferation of biometrics and other data collection in everyday life - for access to banking, essential services, buildings, and cell phones, etc. - can have a corrosive effect on privacy due to the sensitivity of the data collected with proper control or oversight.[19] An example of the danger of insufficient controls for collecting and processing biometric data is how private service providers can lawfully access and

---

[16] See Nicole Ozer and Chris Conley, "After Facebook Privacy Debacle, It's Time for Clear Steps to Protect Users", *American Civil Liberties Union,* 23 March 2018. Available from https://www.aclu.org/blog/privacy-technology/internet-privacy/after-facebook-privacy-debacle-its-time-clear-steps-protect.

[17] Shaohua Li et al, "PPMA: Privacy-Preserving Multisubset Data Aggregation in Smart Grid", *IEEE Transactions on Industrial Informatics*, vol. 14 (2 February 2018).

[18] Ann Cavoukian, "Privacy controls must be placed back into the hands of the individual" *Globe and Mail*, 27 March 2018. Available from https://www.theglobeandmail.com/opinion/article-privacy-controls-must-be-placed-back-into-the-hands-of-the-individual/.

[19] Yue Liu, "Privacy Regulations on Biometrics in Australia", *Computer Law & Security Review,* vol. 2, No. 6 (2010).

monetise the information stored within the South African Department of Home Affairs' biometric registry to market biometric verification technologies.[20]

APPROACHES TO ADDRESS PRIVACY CHALLENGES IN DATA DRIVEN TECHNOLOGY

Proper technical understanding informing the regulation of the technology is the key. Without this understanding by the relevant decision makers it is near impossible to create fit for purpose regulation. This applies to multilateral and national levels of regulation of biometrics collection and big data collection and analysis to ensure that privacy and other human rights considerations are central to the development and implementation of new solutions. We also observe that relying on legal mechanisms alone won't guarantee privacy unless we provide clear guidance to the builders of data driven technology.

With this observation, the standardised, coordinated principles regarding biometric collection, use and retention must include regulatory controls generally, beyond standard contracting. These should at minimum reflect the protective requirements of the General Data Protection Regulation (GDPR) (EU) 2016/679. Under the GDPR, biometrics is one of the "special categories of personal data" given protections at Article 9 of the GDPR. We endorse as a minimum the requirements imposed by this regulation regarding portability, consent, notice, and algorithmic and user-centric transparency.[21]

III. Undue interferences with the right to digital privacy for vulnerable groups

Surveillance, by states and private sector bodies alike, is often disproportionately targeted at the marginalized and vulnerable; this has long been true in physical space, and may be intensified in digital space. Women and girls, religious minorities, people living in poverty, racial and ethnic groups as well as members of indigenous communities, individuals of different genders and all ages may experience similarly disproportionate privacy impacts as a result. The undue interference that digital

[20] An example is the identity verification services offered by IDEMIA. Available from http://www.idemia.com.
[21] We support also the evidence presented in the Advanced Report of SPR on Privacy to 72nd Session of the General Assembly; Bart Custers et al "A Comparison of Data Protection Legislation and Policies Across the EU" *Computer Law & Security Review*, vol. 34 (2018), together with the recommendations from the "Centre for Information Policy Leadership, Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR - Centre for Information Policy Leadership GDPR Implementation Project" (19 May 2017).

systems have on marginalized group's privacy rights has been well documented.[22] A non-exhaustive sample of relevant issues is discussed below.[23]

ALGORITHMS AND ALGORITHMIC DECISION-MAKING

It is clear that vulnerable groups already suffering under disproportionate government scrutiny will be further burdened by these algorithmic technologies.[24] Algorithm-based decision making is often touted as objective, but writing unbiased algorithms is difficult and programmers may, by mistake or even by design, build-in misinformation, racism, bias and prejudice "which tend to punish the poor and the oppressed."[25] Potential discrimination is exacerbated by the opacity of the programs, many of which are proprietary, and a social tendency to assume a machine-made decision is more likely to be objective. While there has been significant scholarly and increasingly, policy-focused work directed towards solutions for creating "fair" algorithms, there are no firmly established international standards for audit, accountability, or transparency.[26]

SYSTEMIC BIAS IN HISTORICAL DATA SETS

Algorithms detect patterns in big data sets. However, many historical data sets have built-in biases of years of problematic collection practices.[27] For example, there is concern that biased policing techniques contribute to biased police data. In Canada, an analysis of 10 years' worth of data regarding arrests and charges for marijuana possession, acquired from the Toronto Police Services, revealed black people with no criminal history were three times more likely to be arrested than white people with

---

[22] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (New York, NY; St. Martin's Press, 2018); Safiya, U. Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York, NY; New York University Press, 2018); Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York, NY; Broadway Books, 2017); Joshua R. Scannell, "Broken Windows, Broken Code", *Reallifemag,* August 29, 2016. Available from http://reallifemag.com/broken-windows-broken-code/.

[23] Parts of this submission draw from Jonathan Obar and Brenda McPhail, "Preventing Big Data Discrimination in Canada: Addressing Design, Consent and Sovereignty Challenges, (2018, in press), Centre for International Governance Innovation.

[24] American Civil Liberties Union, "Will Artificial Intelligence Make Us Less Free? Experts Consider How the Growing Use of AI Will Impact Civil Liberties". Available from https://www.aclu.org/issues/privacy-technology/will-artificial-intelligence-make-us-less-free

[25] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York, N;: Broadway Books, 2017) at 3.

[26] See Bruno Lepri et. al., "Fair, Transparent, And Accountable Algorithmic Decision-making Processes: The Premise, the Proposed Solutions, and the Open Challenges" (2017) *Philosophy & Technology* (2017). Available from https://doi.org/10.1007/s13347-017-0279-x; Sorelle A. Fiedler & Christo Wilson (eds)," Proceedings of Machine Learning Research" *Conference on Fairness, Accountability and Transparency*, vol 81 (23-24 February 2018) New York NY, USA. Available from http://proceedings.mlr.press/v81/; Nicholas Diakopoulos & Sorelle Friedler, "How to Hold Algorithms Accountable," *MIT Technology Review* (17 November 2016). Available from https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/.

[27] Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Cambridge, MA; Harvard University Press, 2015).

similar histories.[28] Data on Indigenous communities has also been collected and interpreted with a focus on statistics that reflect disadvantage and negative stereotyping.[29] At the same time, crimes with a particular impact on women including domestic and sexual assault may, because they are historically under-reported, be under-represented in predictive policing models built on existing data.

Biased algorithms, data sets and discriminatory behavior together result in Big Data discrimination. Research clearly demonstrates that vulnerable communities are disproportionately susceptible to Big Data discrimination.[30] Indeed, "Big Data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace"[31] as well as "immigration, public safety, policing, and the justice system."[32]

DIGITALLY FACILITATED HARASSMENT AND ABUSE

Even if algorithms and data sets were without bias, discriminatory behavior by individuals and institutions may be magnified in the digital age. One example is the proliferation of spyware technologies that "are increasingly being repackaged and sold to facilitate domestic violence, stalking, and other forms of technology-facilitated harassment and abuse that threaten the safety of women and girls."[33]

It is not just the technologies others may use, but the platforms on which social life increasingly plays out that facilitate gender-based violence, harassment, and abuse. Women and girls are disproportionately likely to experience "harassment, hacking, denial-of-service attacks, the use of gender-based slurs, the publication of private and

---

[28] Jim Rankin, Sandro Contenta and Andrew Bailey, "Toronto Marijuana Arrests Reveal 'startling' Racial Divide", *The Star,* 6 July 2017. Available from https://www.thestar.com/news/insight/2017/07/06/toronto-marijuana-arrests-reveal-startling-racial-divide.html.

[29] Open North, and British Columbia First Nations Data Governance Initiative, "Decolonizing data: Indigenous Data Sovereignty Primer" (April 2017).

[30] Seeta Gangadharan, Virginia Eubanks and Solon Barocas, "Data and discrimination: Collected essays." (2014). Available from https://www.newamerica.org/oti/policy-papers/data-and-discrimination/; Nathan Newman, "How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population" (2014). Available from https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf; Solon Barocas and Andrew D. Selbst, "Big data's Disparate Impact." *California Law Review,* vol. 104 (2016); Mary Madden, Michele Gilman, Karen Levy and Alice Marwick, "Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans" vol 95, *Washington University Law Review* (2017).

[31] (The White House 2014, p. 3).

[32] Obar and McPhail 2018.

[33] Ronald J. Deibert, Lex Gill, Tamir Israel, Chelsey Legge, Irene Poetranto & Amitpal Singh, Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms.Dubravka Šimonović, November 2, 2017, p. 15. Available from https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf. The entirety of this report is a relevant contribution to the question of privacy impacts on women and girls in the digital age.

identifiable personal information ("doxing"), impersonation, extortion, rape and death threats, electronically enabled trafficking, and sexual exploitation or luring of minors.[34]

CHILLING EFFECT OF SURVEILLANCE

Not only do digital systems operate in a discriminatory manner, but they also have a greater impact on vulnerable groups. For example, Jonathan W. Penney examined the chilling effects of online surveillance and found that younger people and women are more likely to be chilled and are less likely to take steps to resist regulatory actions and defend themselves.[35] Similarly, studies have shown that an overwhelming majority of Muslim-Americans believe that the U.S. government monitors their post-9/11 activities and consequently have changed their use of the Internet.[36]

APPROACHES TO PROTECT VULNERABLE AND MARGINALIZED GROUPS

Addressing these challenges might involve a combination of strategies including:

- Developing international standards for auditing and eliminating biases in algorithms and data sets;
- Modernizing existing privacy and data protection legislation at the State level to ensure its ongoing effectiveness;
- Promoting and regulating accountability for entities that create and use algorithms and data sets;
- Developing and promoting technological literacy and privacy education for vulnerable populations; and
- Initiating and supporting research that brings women's and girl's voices into policy discussions,[37] and a similar initiative focusing on other marginalized and vulnerable populations.

---

[34] Ibid., p. 2; see, as cited in this source, the following : EC, European Institute for Gender Equality, "Cyber Violence Against Women and Girls" (2017). Available from http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls; UN Broadband Commission for Digital Development Working Group on Broadband and Gender, "Cyber Violence against Women and Girls: A Worldwide Wake-Up Call" (2015). Available from http://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf; Linda Baker, Marcie Campbell, and Elsa Barreto, "Understanding Technology-Related Violence Against Women: Types of Violence and Women's Experiences," Centre for Research & Education on Violence Against Women & Children, Learning Network Brief 6 (2013). Available from http://www.learningtoendabuse.ca/sites/default/files/Baker_Campbell_Barreto_Categories_Technology-Related_VAW_.pdf; see personal accounts detailed in Bytes for All (B4A), in partnership with Association for Progressive Communications (APC). Available from http://content.bytesforall.pk/sites/default/files/ViolenceAgainstWomenPakistanCountryReport.Pdf.

[35] Jonathon W. Penney "Internet Surveillance, Regulation and Chilling Effects Online: a Comparative Case Study" *Journal on Internet Regulation,* vol 6 (2017).

[36] Dawinder S. Sidhu, "The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim Americans" *University of Maryland Law Journal,* vol 7 (2007).

[37] A good Canadian example is the E-girls project, led by the research team of Jane Bailey, Valerie Steeves, Jacquelyn Burkell, Priscilla Regan, Madelain Saginur and Jane Tallim, Available from https://egirlsproject.ca/the-project/what-we-are/.

IV. Safeguards against surveillance, processing, and interception of digital communications

The right to privacy may only be limited through a law which regulates infringement. The United Nations General Assembly Resolution on the Right to Privacy in a Digital Age reaffirms the international law principle that no one shall be subject to arbitrary and unlawful interference with their right to privacy.[38] It further calls on states to review their legislation and procedures for lawful surveillance, as well as ensure the existence of independent and effective oversight mechanisms for accountability.[39]

The following principles ought to inform minimum principles for the the design and mandate of government legislations, regulations, and policy:

- Complete institutional independence of oversight bodies, including security of tenure for ex officio staff; full budgetary control; and administrative accountability to the executive, but not for decisions relating to mandated functions;
- Pre-surveillance authorisation from a judicial or quasi-judicial authority, which is not too proximate to the institutions carrying out the surveillance, and only where there is clear evidence of a sufficient threat and the surveillance proposed is targeted, strictly necessary, and proportionate; and
- An effective and accessible remedy for people subjected to unlawful surveillance, including post notification and the possibility of civil compensation and criminal sanction for unlawful surveillance.

While the focus is generally on state led surveillance and the oversight thereof, we note that there is also increasing importance in oversight of and providing remedies against private entities. The extent of data collected by private entities and the private ownership of information infrastructures allows great scope for infringement of the right to privacy by private entities.

V. Concluding remarks and next steps

The above important challenges including encryption and anonymity, reliance on data driven technology, and digital privacy for vulnerable groups might be addressed through further elaboration and authoritative interpretation of existing legal obligations protecting the right to privacy as enshrined in Article 17 of the ICCPR.

The Human Rights Committee is the only relevant U.N. human rights body, to date, not to have taken steps to address digital privacy rights (and state obligations to protect them) in a systematic and comprehensive manner. The Committee's voice on informational privacy is indispensable at this critical time. Through the process of revising General Comment 16, the Committee will have the opportunity to address

[38] The Right to Privacy in a Digital Age UN Resolution A/RES/68/167 at 1.
[39] The Right to Privacy in a Digital Age UN Resolution A/RES/68/167 at 2.

these urgent issues outlined for the purpose of this report. The Committee will also have the opportunity to reestablish itself as a leading body in the protection of privacy - what is now recognized as one of the world's most widely violated human rights and which is critically vulnerable in a digital age.

By contrast, in the absence of input from the Committee, states will continue to rely on dated standards both when reporting to the Committee on compliance with the ICCPR and in defending individual petitions, thereby undermining the proper development of international law. The general comment revision process—and the revised general comment that results—will also assist other U.N. and regional bodies, as well as national legislatures and courts, as they formulate laws, policies and practices that embrace relevant ICCPR privacy standards.

INCLO is a network of 13 independent, national human rights organizations from the global South and North. We work together to promote fundamental rights and freedoms.