The right to privacy in the digital age
Human Rights Council adopted resolution 34/7
April 2018

Introduction

The International Network of Civil Liberties Organisations (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 and of opinion. These rights are enshrined in international human rights law and are recognized as deserving of strong protections through encryption protocols. 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. Anonymous communications afforded by encryption technologies provide advantages to populations who are discriminated against by providing them safe forums to congregate, organize, mobilize, and build community. Currently, these encrypted safeguards tend to be under attack in certain states which attempt to either block access to or intercept encryption protocols.

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, governments and intelligence agencies have attempted to encroach upon this right. A lack of respect for anonymous communications rights assists government justification for accessing the content and communications

---

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.
4 The Egyptian LGBTQ community increasingly relies on encrypted communications like Signal; ibid.
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.”
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 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 emails13 and government agencies housing the personal information of


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.
citizens\textsuperscript{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.\textsuperscript{15}

**Addressing these challenges**

While the rights to privacy and to freedom of expression 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
- 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.\textsuperscript{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.\textsuperscript{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

\textsuperscript{14} See for example the global ransomware attack that crippled the NHS and the hack of India’s Aadhaar database.

\textsuperscript{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.


technology to allow individuals to control their own set of personal data. 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 without proper control or oversight. An example of the danger of insufficient controls for collecting and processing biometric data is how private service providers can lawfully access and monetise the information stored within the South African Department of Home Affairs' biometric registry to market biometric verification technologies.

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.

---

20 An example is the identity verification services offered by IDEMIA. Available from http://www.idemia.com.  
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 systems have on marginalized group’s privacy rights has been well documented. 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 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.”\(^{33}\)


\(^{29}\) Open North, and British Columbia First Nations Data Governance Initiative, “Decolonizing data: Indigenous Data Sovereignty Primer” (April 2017).


\(^{31}\) (The White House 2014, p. 3).

\(^{32}\) Obar and McPhail 2018.

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 identifiable personal information (“doxing”), impersonation, extortion, rape and death threats, electronically enabled trafficking, and sexual exploitation or luring of minors.\textsuperscript{34}

\textbf{Chilling effect of surveillance}

Not only do digital systems operate in a discriminatory manner, but they also have a greater impact on vulnerable and marginalized 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.\textsuperscript{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.\textsuperscript{36}

\textbf{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, and a similar initiative focusing on other marginalized and vulnerable populations.

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. 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.

The following principles ought to inform minimum principles for 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.

---

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/.
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.
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 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.

Contact: Elizabeth Farries, INCLO Information Rights Program Manager, elizabeth.farries@iccl.ie