UN Special Rapporteur on Freedom of Peaceful Assembly and Association Call for Inputs: HRC47th Session Report on Accountability & Access to Justice in the Context of FoAA

2 February 2021

Introduction

Access Now welcomes this opportunity to provide relevant information to the United Nations (U.N.) Special Rapporteur on Freedom of Peaceful Assembly and Association (the Special Rapporteur) to inform the Special Rapporteur's report to be presented at the 47th session of the Human Rights Council on Accountability and Access to Justice in the context of the rights to freedom of peaceful assembly and of association.[1] As an ECOSOC accredited organisation, Access Now routinely engages with U.N. Special Procedures in support of our mission to extend and defend digital rights of users at risk around the world.[2]

Access Now is pleased to provide input on the Special Rapporteur's thematic report by offering a digital perspective to the questions posed. This submission focuses on the following: (I) privacy enhancing measures like encryption as a vital tool to ensure lawyers better support those exercising their right to freedom of peaceful assembly, (II) how the Special Rapporteur can build on his previous calls for protection of encryption in digital technologies in the context of freedom of peaceful assembly, and (III) targeting of legal observers (*i.e.* monitors) in the context of peaceful Black Lives Matter demonstrations in the United States (U.S.).

I. Measures that could be taken to help lawyers better support those exercising their right to freedom of peaceful assembly

I. I. Promoting and defending lawyer's use of encryption, and other digital security features, in lawyer-client communications

The legal profession has largely failed to adapt to technological change in the past few decades, and remains particularly at risk of privacy violations and digital security threats. This digital insecurity impacts those most vulnerable individuals and entities — clients, witnesses, defendants, and petitioners — with whom lawyers interact. Despite mounting evidence of surveillance, manipulation, disruption, and reprisal levied against lawyers through digital means, most have yet to adopt basic

[1] OHCHR, Call for inputs from the Special Rapporteur on the rights to freedom of peaceful assembly and of association for his report to be presented at the 47th session of the Human Rights Council, 2021, available at https://www.ohchr.org/EN/Issues/AssemblyAssociation/Pages/HRC47Report.aspx

[2] Access Now, About Us, 2021, available at https://www.accessnow.org/. 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. Access Now works to defend and extend the digital rights of users at risk around the world through policy, advocacy, technology support, grants, legal interventions, and global convenings like RightsCon.

technological safeguards or girded their workflows to deflect attacks. The profession must take responsibility for its digital footprints, and states must encourage – not hamper – such efforts.

Encouraging digital security and defending a lawyer's use of encryption is vital for the profession to better support their clients who are exercising their right to freedom of peaceful assembly while also affirming the right to attorney-client privilege and maintaining a lawyer's professional obligations. Encryption protects the confidentiality and integrity of digital files and communications by creating a "zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks."[3] Practically speaking, encryption makes data unreadable except to the person who has the "key" to "decrypt" the encrypted data or device — be it a message, file, or disk — into readable form.[4] End-to-end encryption affords even more robust protection as it "protects the message in transit all the way from sender to receiver."[5]

Overall, tools such as encryption, multi-factor authentication, and other digital security features empower individuals to operate safely in digital spaces to connect and mobilize, without undue interference, and confidentially communicate with their legal counsel for advice. As the former U.N. Special Rapporteur of Freedom of Opinion and Expression, David Kaye recognized, "anonymous speech has been necessary for activists and protesters, but States have regularly attempted to ban or intercept anonymous communications in times of protest."[6] Third parties, such as social media, spyware and other tech companies also can collect and store data on associations and those assembling online and off. For instance, spyware companies may sell or share this information to other third parties, including police authorities. According to research conducted by the Citizen Lab, NSO Group's Pegasus spyware has been used in 45 countries, with at least six countries with significant Pegasus operations having been previously linked to the abusive use of spyware to target civil society, human rights defenders, and those engaging in protests.[7]

Robust encryption is therefore essential in the context of peaceful protests — specifically when a lawyer's advice is solicited and triggers other rights and protections, as it aims to protect networks and

---

[3] U.N. Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, U.N. Doc. A/HRC/29/32, 22 May 2015, available at https://undocs.org/A/HRC/29/32 , at paras 3, 6. For more information on encryption generally see: EFF, Surveillance Self Defense, What You Should Know About Encryption, 24 November 2018, available at https://ssd.eff.org/en/module/what-should-i-know-about-encryption#:~:text=End%2Dto%2Dend%20encryption%20protects,the%20second%20%E2%80%9Cend%E2%80%9D)

[4] EFF, Surveillance Self Defense, What You Should Know About Encryption, 24 November 2018, available at https://ssd.eff.org/en/module/what-should-i-know-about-encryption#:~:text=End%2Dto%2Dend%20encryption%20protects,the%20second%20%E2%80%9Cend%E2%80%9D)

[5] *Ibid.*

[6] U.N. Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, U.N. Doc. A/HRC/29/32, 22 May 2015, available at https://undocs.org/A/HRC/29/32 , at para 53 cited in Access Now, Defending Peaceful Assembly and Association in the Digital Age, July 2020, available at: https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf

[7] The Citizen Lab, Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, 2018, available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ cited in Access Now, Defending Peaceful Assembly and Association in the Digital Age, July 2020, available at: https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf

data from unauthorized surveillance, particularly from law enforcement and other government agencies.[8]

I. II. Compounded surveillance of those who face marginalization on the basis of intersecting identities

Surveillance and censorship risks are compounded for those who face marginalization through intersecting identities, whether on the grounds of race, ethnicity, sexual orientation, religion, or otherwise. The U.N. Special Rapporteur on Racism, E. Tendayi Achiume, has highlighted that authorities increasingly use invasive surveillance technologies, in some cases intended for purposes such as border control, against people in Black and Latinx communities who are targeted for discrimination and racist attacks.[9] For instance, according to the Brennan Center for Justice, the Department of Homeland Security in the U.S. "has reportedly used its social media monitoring programs to surveil Black Lives Matter activists, individuals involved in anti-Trump protests in New York City, and lawyers and journalists at the southern border."[10]

As evidenced above, third parties and authorities, including law enforcement and government agencies, routinely abuse surveillance tools to monitor lawful protests. While protesters, particularly those from marginalized communities, are more susceptible to surveillance, when someone exercising their right to peaceful protest is detained, arrested or otherwise in police custody, their likelihood of surveillance, particularly by law enforcement agencies increases. Calls and messages from prison are in many cases routinely surveilled, and are even leaked to the public.[11] Action at the international level must be taken to defend and encourage encryption for all attorney-client conversations to ensure that individuals, especially those already suffering from systemic racism, discrimination, and abuse are not further stripped of their fundamental rights and freedoms.[12]

I.III. Surveillance of lawyer-client communications in the U.S. — the case for encryption

Consider the U.S. case of Gerard Howard, who was arrested on suspicion of possession of heroin and drug paraphernalia. In Howard's case, the police never found illegal drugs on him, but seven minutes into a confidential toll-free call from his jail cell to his attorney, he said "just like after detox or whatever…they just moved me to a different building." The New Orleans District Attorney then used the jail's recording of the call — specifically citing Mr. Howard's use of the word 'detox'— as the key element of the crime of 'possession of drug paraphernalia' in order to convict and sentence him."[13] In

[8] Access Now, Encrypt All the Things, available at https://www.encryptallthethings.net/ last accessed 2 February 2021.
[9] Access Now, Encryption is vital for attorney-client privilege in the digital era, and lawyers should fight for it, 11 January 2021, available at https://www.accessnow.org/encryption-attorney-client-privilege/.
[10] Brennan Center for Justice, Government: Social Media Surveillance, available at https://www.brennancenter.org/issues/protect-liberty-security/social-media/government-social-media-surveillance last accessed 2 February 2021.
[11] Access Now, Encryption is vital for attorney-client privilege in the digital era, and lawyers should fight for it, 11 January 2021, available at https://www.accessnow.org/encryption-attorney-client-privilege/ ; Tech Crunch, A prison video visitation service exposed private calls between Inmates and their attorneys,10 October 2020, available at https://techcrunch.com/2020/10/10/prison-visitation-homewav-leak/
[12] Access Now, Encryption is vital for attorney-client privilege in the digital era, and lawyers should fight for it, 11 January 2021, available at https://www.accessnow.org/encryption-attorney-client-privilege/
[13] *Ibid.*

an interview with *the Guardian*, Howard's attorney, Thomas Frampton, said the call ended up being the "centerpiece of their case against my client."[14] He also said prosecutors had "no other evidence to meet their burden of proving that the needle in his pockt qualified as 'paraphernalia' under Louisiana law."

Howard's case is situated in a larger context of prison surveillance throughout the U.S. Indeed, U.S. prison authorities continue to undermine people's Sixth Amendment right — a right to privacy of communication with legal counsel — by recording attorney-client communications on a massive scale. This information is publicly known because companies that provide prison telecom services are making mistakes and exposing people's private conversations. For instance, HomeWAV, a company used in dozens of prisons across the U.S to provide prisoners with phone services, left an unsecured database exposed to the internet from April to October 2020. HomeWAV's representatives have refused to explain why the company recorded and transcribed these conversations when they are supposed to be protected by attorney-client privilege.[15]

Lawyers and lawyer associations must advocate for better digital security standards, and help push regulations to strictly limit surveillance and protect individuals' rights. The American Bar Association already encourages attorneys to protect digital communications and their clients' data, including through encryption and technological due diligence.[16] Local and state bar associations are updating ethics rules, including in Texas,[17] and providing training resources to improve digital security skills.[18] Yet a 2019 survey shows that "less than half of respondents use file encryption (44%), slightly more than a third use email encryption (38%)."[19] These figures are particularly shocking when compared to those of professional journalists. Both attorneys and journalists have similar professional obligations to provide confidentiality to clients and sources. But unlike attorneys, more than two-thirds of journalists and newsrooms use end-to-end encryption tools and most major print media, from *The New York Times* to *USA Today* to *The Intercept*, offer open source encrypted drop boxes for first contact with sources. These facts make it clear that attorneys need stronger guidance from their regulators.[20]

I. IV. Government responses to the use of encryption and other digital security features

[14] Access Now, Encryption is vital for attorney-client privilege in the digital era, and lawyers should fight for it, 11 January 2021, available at https://www.accessnow.org/encryption-attorney-client-privilege/ ; The Guardian, 'Plainly unconstitutional': New Orleans jail records inmates' calls to lawyers, 22 May 2018, available at https://www.theguardian.com/us-news/2018/may/22/new-orleans-prison-phone-calls-attorney-client-privilege

[15] Access Now, Encryption is vital for attorney-client privilege in the digital era, and lawyers should fight for it, 11 January 2021.

[16] American Bar Association, Formal Opinion 477: Securing Communication of Protected Client Information, 11 May 2017, available at https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf

[17] State Bar of Texas, Opinion No. 648 Under the Texas Disciplinary Rules of Professional Conduct, may a lawyer communicate confidential information by email? April 2015, available at https://www.texasbar.com/AM/Template.cfm?Section=Past_Issues&Template=/CM/ContentDisplay.cfm&ContentID=30523

[18] State Bar of Texas, Opinion No. 648 Under the Texas Disciplinary Rules of Processional Conduct, may a lawyer communicate confidential information by email? April 2015, available at https://www.texasbar.com/AM/Template.cfm?Section=Past_Issues&Template=/CM/ContentDisplay.cfm&ContentID=30523

[19] American Bar Association, 2019 Cybersecurity, 16 October 2019, available at https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity2019/

[20] ICFJ, The State of Technology in Global Newsrooms, 2019, available at: https://www.icfj.org/sites/default/files/2019-10/2019%20Final%20Report.pdf ; SecureDrop, Directory, 2021 available at https://securedrop.org/directory/

Some governments claim that technologies that enable users to communicate securely and protect their private information, like encryption, pose threats to national security, particularly in the context of protests. For instance, Ethiopian officials jailed six bloggers in part because they took part in digital security training designed to teach users to use basic encryption.[21] Similarly, Spanish authorities arrested eleven people who were using "extreme security measures" including encrypted email,[22] and Turkish authorities arrested and held digital security trainers without access to their lawyers.[23] These examples are situated in a larger context where governments are implementing policies to require "backdoors" through encryption protocols *i.e.* intentional vulnerabilities granting access to users' information or that force users to link their real identities to their online speech.[24] Such invasive policies restrict individual's right to privacy and demonstrably chill online free speech.

More recently, governments have shown more promising commitments to secure and protect the confidentiality of digital communications through encryption. These governments are also encouraging business enterprises to work towards enabling such technologies. On 6 December 2020, the U.N. General Assembly adopted by consensus a new resolution on privacy in the digital age. The resolution, which was co-led by Brazil and Germany, and co-sponsored by a record cross-regional group of 69 countries, reaffirms the fundamental importance of the right to privacy and renews international commitment to ending all abuses and violations of this vital human right.[25] In 2017, this was the first U.N. resolution to discuss encryption and its importance to human rights. However, the 2020 version of this resolution takes a step further, with a positive call to "enact policies" around encryption and anonymity that "recognize and protect the privacy of individuals' digital communications."[26]

Nonetheless, with more targeted attempts to weaken encryption and erode anonymity stronger than ever, this strengthened language in the U.N. General Assembly Resolution sends a strong signal to the international community about the fundamental importance of encryption and anonymity for the realization of human rights.[27] These technologies allow individuals to express themselves without fear of reprisal and ensure access to information, especially in those countries where the right to freedom of expression is under threat. This is particularly the case for groups at-risk of discrimination and violence.

---

[21] Pen American Center, Encryption and the Faustian Bargain, 15 August 2014, available at http://www.pen.org/blog/encryption-and-faustian-bargain
[22] RiseUp, Security is not a Crime, 6 January 2015, available at https://help.riseup.net/en/aboutus/press/security-not-a-crime
[23] EFF, EFF Condemns Detentions at Turkish Digital Security Meeting, 6 July 2017, available at https://www.eff.org/deeplinks/2017/07/eff-condemns-detentions-turkish-digital-security-meeting
[24] Access Now, Governments want encryption backdoors: new report examines the legal and policy implications, 14 February 2018, available at https://www.accessnow.org/governments-want-encryption-backdoors-new-report-examines-legal-policy-implications/
[25] Access Now, To Protect Privacy in the digital Age, World Governments Can and Must do More, 25 January 2021, available at https://www.accessnow.org/un-privacy-resolution/
[26] *Ibid.*
[27] Schneier, G7 Outcomes in Favor of Encryption Backdoors, 23 April 2019, available at https://www.schneier.com/blog/archives/2019/04/g7_comes_out_in.html

II. How the Special Rapporteur can contribute to greater accountability for violations of the rights to FoAA and concretely contribute to ensuring effective access to justice of persons exercising these fundamental freedoms

The Special Rapporteur should build upon his previous efforts[28] and echo previous and recent calls for encryption and anonymity at the Human Rights Council as a means to enable peaceful protesters seeking legal advice to exercise their human rights, and therefore encourage strong protection of this and other vital digital security tools.[29] The Special Rapporteur should highlight and take advantage of the governmental momentum on encryption as captured in the recent U.N. General Assembly Privacy Resolution to advance international norms on the intersection of the right to privacy and freedom of peaceful assembly while also underpinning the importance of digital security tools for lawyer-client communications.

Effective access to justice requires timely legal advice. Digital communications — particularly during social distancing measures as a result of COVID-19 — are essential to ensuring lawyer's provide timely legal advice to their clients. We therefore must push to strengthen the privacy and security of lawyer-client communications as a means to strengthen access to justice, specifically timely legal services.

To address the proliferation of surveillance technology, which is often misused against those exercising their rights to association and peaceful assembly, the Special Rapporteur can join the joint call for a moratorium "on the global sale and transfer of private surveillance technology," as declared by the Special Rapporteurs on the freedoms of expression and opinion, summary executions and extrajudicial killings,[30] and on racism and xenophobia,[31] and joined by the U.N. High Commissioner for Human Rights.[32]

III. Lawyers participating in peaceful assemblies as legal observers — targeting in the U.S.

III.I. Legal Observers and Peaceful Protests in the U.S.

Legal observers worldwide serve to monitor and report law enforcement conduct during peaceful protests. The extrajudicial killing of George Floyd on 25 May 2020, an unarmed Black man in Minneapolis, Minnesota, sparked national and global demonstrations calling attention to and condemning structural racism and police brutality. The former U.S. Government responded to these

---

[28] U.N. Human Rights Council, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clement N. Voule, U.N. Doc. A/HRC/41/41, 17 May 2019, available at https://undocs.org/A/HRC/41/41

[29] Most notably, U.N. Human Rights Council, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clement N. Voule, U.N. Doc. A/HRC/41/41, 17 May 2019, available at https://undocs.org/A/HRC/41/41 at paras 24, 35, 55, 73(d); U.N. Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, U.N. Doc. A/HRC/29/32, 22 May 2015, available at https://undocs.org/A/HRC/29/32 , at paras 12, 56.

[30] *See* OHCHR, UN experts call for investigation into allegations that Saudi Crown Prince involved in hacking of Jeff Bezos' phone, 22 January 2020, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25488

[31] *See* OHCHR, UN expert joins call for immediate moratorium on sale, transfer and use of surveillance tech, 15 July 2020, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26098&LangID=E

[32] *See* U.N. Human Rights Council, Annual Report of U.N. High Commissioner for Human Rights, U.N. Doc. A/HRC/44/24, 24 June 2020 at para 40.

peaceful demonstrations by deploying militarized police forces into communities without state or local official invitation or authorization. These forces have used excessive and discriminatory force, arbitrarily detained legal observers and generally suppressed their freedoms of expression and opinion, association and assembly, and the right to privacy in major U.S. cities.[33]

III.I.I. Surveillance & Treatment of Legal Observers in the U.S.

As noted above, third parties and authorities, including law enforcement and government agencies, routinely abuse surveillance tools to monitor lawful protests. The U.S. is no exception to this. From local police to the federal government, authorities abused surveillance tools to monitor lawful political activity during the protests. Examples show the repurposing of tools intended for other ends: the Department of Homeland Security's use of drones, airplanes, and helicopters purchased for its customs and border enforcement to instead monitor Black Lives Matter protests in more than 15 cities, [34] video footage captured by "smart streetlights" in San Diego, installed to monitor traffic and environmental conditions, used instead to persecute protesters,[35] and social media monitoring and police procurement of Twitter data regarding protests, including the location data of peaceful demonstrators.[36] The Washington Post also reports that the U.S. Department of Homeland Security has accessed protesters' electronic messages and has been regularly monitoring such messages and compiling them in an "intelligence report."[37]

In the U.S., legal observers, in addition to volunteer medics and journalists, reporting live from peaceful Black Lives Matter demonstrations have also been the target of brutal police forces. On 4 August 2020, Amnesty International U.S.A. released a detailed report titled *USA: The World is Watching: Mass Violations by U.S. Police fo Black Lives Matter Protesters' Rights* (the Report). The Report documents "the widespread and egregious human rights violations by [U.S] police officers against … legal observers who gather to protest the unlawful killings of Black people by the police and to call for systemic reform in May and June of 2020."[38] It contains a dedicated section on "Targeting of Legal

[33] On 4 December 2020, the University of Southern California Gould School of Law International Human Rights Clinic and Access Now, with the support of Foley Hoag LLP submitted relevant information to the U.N. High Commissioner for Human Rights for consideration for her report to the Human Rights Council's (HRC) 47th Session in June 2021 pursuant to HRC Resolution A/HRC/RES/43/1 on the "Promotion and protection of the human rights and fundamental freedoms of Africans and of people of African descent against excessive use of force and other human rights violations by law enforcement officers."This section therefore provides a summary of the relevant information specifically regarding legal observers from the submission for the Special Rapporteur's consideration. While the U.S. has since had a change in its federal administration, the information is still relevant to inform the Special Rapporteur's report. More information available at https://www.accessnow.org/cms/assets/uploads/2020/12/USCAccess-Now-OHCHR-Submission-4.12.20.pdf

[34] The New York Times, U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance, 19 June 2020, available at https://www.nytimes.com/2020/06/19/us/politics/george-floydprotests-surveillance.html

[35] The City of San Diego, San Diego to Deploy World's Largest City-Based 'Internet of Things' Platform Using Smart Streetlights, 22 February 2017, available at https://www.sandiego.gov/mayor/news/releases/sandiego-deploy-world%E2%80%99s-largest-city-based-%E2%80%98internet-things%E2%80%99-platformusing-smart ; See also Mashable, "Police Used 'Smart Streetlights' To Surveil Protesters, Just As Privacy Groups Warned," 30 June 2020, available at https://mashable.com/article/police-surveil-black-livesmatter-protesters-smart-streetlights

[36] The Intercept, "Police Surveilled George Floyd protests with help from Twitter-affiliated startup Dataminr," 9 July 2020, available at https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/ See also Brookings, "How to reform police monitoring of social media" 9 July 2020, available at https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.

[37] The Washington Post, DHS Analyzed Protester Communications Despite Comments to the Contrary, 31 July 2020, available at https://www.washingtonpost.com/nation/2020/07/31/protests-live-updates/.

[38] Amnesty International USA, USA: The World is Watching: Mass Violations by U.S. Police of Black Lives Matter Protesters' Rights, 2020, available at https://www.amnestyusa.org/wp-content/uploads/2020/07/WorldisWatchingFullReport080220.pdf; *See* also National Lawyers

Observers" in this context.[39] In this section, the Report indicates several instances in which legal observers were targeted and brutally attacked or arrested. In one instance, a woman was grabbed from the back of her hands and were zip-tied to her back as she was walking away from a line of protesters. In another instance, an officer told a legal observer that he did not need to advise the woman of her rights because he was not interrogating her.[40]

III.I.II. Protection of Legal Observers under the U.S. First Amendment

The First Amendment of the U.S. Constitution guarantees the freedoms of speech and of the press. Even if a demonstration becomes unlawful or is dispersed, legal observers should still have the right to monitor, report, record, and provide care at demonstrations. Legal observers and volunteer medics remain neutral at demonstrations and should not be targeted by law enforcement. Legal observers attend protests to monitor and document police conduct and violations of protesters' legal rights. They typically wear gear, such as hats or shirts, to signal to police that they are observers. Like journalists, legal observers and medics' First Amendment rights should not be restricted by law enforcement officers when participating in peaceful protests.

Various civil society groups and individuals have turned to U.S. courts in response to police violence and brutality of legal observers during peaceful demonstrations. On 28 June 2020, the American Civil Liberties Union, on behalf of journalists and legal observers covering protests following George Floyd's killing in Portland, Oregon filed a class action lawsuit against the City of Portland and its police officers.[41] On 23 July 2020 a Portland judge issued a temporary restraining order stating police cannot arrest, threaten to arrest or use force against a person who they know to be a journalist or legal observer.[42]

Recommendations

As state and corporate actors continue to maximize data collection and retention, governments worldwide must take concrete measures to address existing and emerging threats to affirm and safeguard the fundamental human right to privacy. The 2020 U.N. General Assembly Privacy Resolution presents a ripe opportunity for the Special Rapporteur to urge all states to act on their recommendations and enact laws which explicitly recognize that individuals, including lawyers and their clients, are free to protect the privacy of their digital communications by using encryption

---

Guild, Police Targeting NLG Legal Observers at Black Lives Matter Protests, 7 June 2020, available at https://www.nlg.org/police-targeting-nlg-legal-observers-at-black-lives-matter-protests/

[39] Amnesty International USA, USA: The World is Watching: Mass Violations by U.S. Police of Black Lives Matter Protesters' Rights, 2020, available at https://www.amnestyusa.org/wp-content/uploads/2020/07/WorldisWatchingFullReport080220.pdf; at page 48.

[40] Amnesty International USA, USA: The World is Watching: Mass Violations by U.S. Police of Black Lives Matter Protesters' Rights, 2020, available at https://www.amnestyusa.org/wp-content/uploads/2020/07/WorldisWatchingFullReport080220.pdf; at pages 49-52.

[41] *See* ACLU Oregon, ACLU of Oregon Files Class Action Lawsuit against Police in Portland for Attacking Journalists and Legal Observers, 28 June 2020, available at https://aclu-or.org/en/press-releases/aclu-oregon-files-class-action-lawsuit-against-police-portland-attacking-journalists ; see also legal complaint available at https://aclu-or.org/sites/default/files/field_documents/woodstock_portland_aclu_or_06282020.pdf

[42] NPR, Order Temporarily Blocks Feds from Targeting Press and Legal Observers in Portland, 23 July 2020, available at https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/07/23/894953202/order-temporarily-blocks-feds-from-targeting-press-and-legal-observers-in-portla ; see also the restraining order available at https://www.courtlistener.com/recap/gov.uscourts.ord.153126/gov.uscourts.ord.153126.84.0.pdf

technology and tools that allow anonymity online. We therefore respectfully request that the Special Rapporteur make the following observations and recommendations for your report on Accountability and Access to Justice in the context of the rights to freedom of peaceful assembly and of association to be presented at the 47th session of the Human Rights Council:

1. Protect and promote privacy-enhancing technologies specifically in the context of attorney-client communications, and safeguard people's use of encryption, pseudonymity, and anonymity, essential enablers of human rights;
2. Urge all states to act on the recommendations in existing resolutions and reports, including but not limited to this Special Rapporteur's 2019 Human Rights Council Report, the former Special Rapporteur on Freedom of Opinion and Expression, David Kaye's 2015 Human Rights Council Report, and the 2020 U.N. General Assembly Privacy in the Digital Age Resolution;
3. Join the call for a moratorium on the transfer, sale, and use of private surveillance technology;
4. Call on states to enact laws which explicitly recognize that individuals, including lawyers and human rights defenders, are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online;
5. Call on lawyers' and judges' associations and accreditation bodies to promote attention to the risks and opportunities of lawyering in the digital age, with special attention to the digital security threats facing jurists and their clients, staff, and contacts involved in peaceful assembly and association; and to provide resources and training to counter such risks;
6. Call on the private sector to protect user privacy and security through data minimization policies, the encryption and anonymization of user data, and the transmission of user data over encrypted channels, whenever and wherever possible;
7. Call on the U.N. to evaluate and strengthen existing digital security and encryption tools used in information technology initiatives like the U.N. Secretary-General's Data Strategy;
8. Highlight in your Report the widespread human rights violations in the U.S. against legal observers as noted in this submission;
9. Protect the rights of legal observers, including the right to monitor and report law enforcement conduct.

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

*For more information, please contact: **un@accessnow.org***