Professor Philip Alston

Mandate of the Special Rapporteur on Extreme Poverty and Human Rights

Office of the High Commissioner for Human Rights

UNOG-OHCHR, CH1211 Genève 10, Suisse

Sept. 19, 2017

Re: Special Rapporteur on extreme poverty and human rights: Country visit to the United States

To Professor Philip Alston, Special Rapporteur on EPHR,

We write to you to express our appreciation of your forthcoming visit to the United States, and to offer input on dimensions of poverty in the U.S. that intersect with human rights in the digital sphere.

Access Now is an international organization that defends and extends the digital rights of users at risk. Digital rights violations are an emerging method to further oppress impoverished populations, in the U.S. as elsewhere. We encounter intersections between poverty and digital rights often in our work, and highlight several areas for the Special Rapporteur: network discrimination and economic or infrastructural barriers to online access; legal barriers which enforce conditions of poverty due to large collections of private data; and the proliferation of electronic surveillance targeting at risk communities.

To answer the Special Rapporteur’s first question, we agree with the OHCHR definition, that “[p]overty is not solely an economic issue, but rather a multidimensional phenomenon that encompasses a lack of both income and the basic capabilities to live in dignity.”[[1]](#footnote-1) This interpretation reflects the nature of modern attacks on individuals’ rights and well-being: human rights violations are often multi-faceted abuses which disproportionately affect vulnerable populations already suffering marginalization.

Unfortunately, the United States continues to define poverty as solely a financial obstacle, which is borne of factors contributing to an individual’s or family’s yearly income.[[2]](#footnote-2) This incomplete understanding of the factors of modern poverty impacts the lives of more than the roughly forty-five million United States residents officially recognized as living below the “poverty line” in ways other than their economic wellbeing. Below, we will describe how this influence manifests in limitations on the digitial rights of these impoverished people in the United States.

**Access to the open internet**

Those living in poverty in the United States face enormous obstacles in obtaining adequate network access. Internet service providers (ISPs) have scaled their infrastructure impressively in recent years, but have continued to neglect user groups with low income rates. For example, the Center for Public Integrity found “even though Internet access has improved in recent years, families in poor areas are almost five times more likely not to have access to high-speed broadband than the most affluent American households.”[[3]](#footnote-3)

Historically, ISPs have reported that they do not include population statistics such as income or racial composition when selecting zones to extend their service. Rather, they include regions in their network based on population density. However, for those living in rural areas (on average median income for rural Americans is 4% lower than that of urban Americans)[[4]](#footnote-4) internet access is still severely limited by demographic factors.[[5]](#footnote-5)

Due to low demand for internet connection in these regions, ISPs are able to impose relatively exorbitant rates for access to their network. According to experts, “[t]hat leaves tens of millions of Americans with the choice of either purchasing an expensive connection from the only provider in their area, typically a cable company, or just doing the best they can with slower speeds.”[[6]](#footnote-6)

It is no coincidence that the richest states in the country are also some of the most well connected to online services. New Jersey, and Connecticut are the two top states in the FCC’s National Broadband Map ranking of the nation’s fastest internet speeds, and are also ranked fourth and fifth respectively in median household income.[[7]](#footnote-7) Poor states are also disadvantaged in access to a variety of service providers. Arkansas is the second poorest state in the country, as well as the third worst state in representation of ISPs. States such as Arkansas, Mississippi, and West Virginia all fare poorly in wealth and internet connection indexes, and would be ideal locations for the Special Rapporteur to visit in order to understand the obstacles to connectivity in impoverished communities.

However, even if an individual living in poverty is able to make use of a provider’s network, they still face obstacles in obtaining adequate service. One of the newest threats to impoverished populations’ access to online content lies in so-called “zero rating” business models. Zero rating programs manifest in different forms. In the telco model, implemented by companies like Verizon, the provider gives preferential treatment to its own content or content of participating third parties, over other content that might use its network.[[8]](#footnote-8) The second, and much more restrictive, model is sub-internet offers, where only part of the internet — a tightly controlled “walled garden” network — is free. Here, tech companies insert themselves in the middle of all communications in partnership with a telecom carrier, and dictate everything that users can and cannot do within the zero rated walled garden. With current implementations of this model, users cannot engage with any website or service without the provider of the zero rated service seeing their traffic and knowing what they are doing.

**Zero rating: free data with a high cost**

In the May 2017 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,the Special Rapporteur David Kaye explored the human rights impacts of zero rating programs on at-risk user groups:

Variations notwithstanding, zero rating arrangements privilege access to content and may increase the cost of metered data. For users who struggle to afford metered data, they might end up relying exclusively on zero-rated services, resulting in limited access to information for communities that may already be marginalized in their access to information and public participation..[[9]](#footnote-9)

“Sub-internet” offers are marketed as inclusive of populations with limited online access, for example by Facebook in the description of the Free Basics program, *“[b]y introducing people to the benefits of the internet through these services, we hope to bring more people online and help improve their lives.”*[[10]](#footnote-10) However, recent research published by the Alliance for Affordable Internet (A4AI), found that “zero rating did not bring most mobile internet users online for the first time.”[[11]](#footnote-11)

Limiting access to the full internet materially impacts low income users, who prefer even short-term or low-bandwidth access to an open, unrestricted internet, over the restricted experience that zero rating provides.[[12]](#footnote-12) If this business model takes hold, poorer users may only be able to participate in online interactions hosted by companies that provide them with their free service. This effective monopolization of service causes severe obstacles to political and civil online discourse for those who can not afford a typical ISP.[[13]](#footnote-13)

Recent proposed rule changes by the FCC will likely cause these restrictions to grow, with threats to net neutrality becoming increasingly relevant.[[14]](#footnote-14) While an open internet benefits everyone, those in poverty stand to lose the most if service providers continue to leverage their hold on users access to an affordable and accessible online presence.

**Big data, surveillance, and poverty**

While users in poverty face restrictive conditions online imposed by their service providers, they must also endure invasive collection and retention of their private data by state and federal governments, as well as other agencies.

Immigrants to the United States, who often travel to the country in pursuit of bettering their economic circumstance, have been placed under an enormous amount of scrutiny in recent years, and are often the first to be targeted with emerging surveillance technology and methods. Legal and undocumented immigrants to the United States are regularly exposed to biometric data requests that are otherwise reserved for counter-terrorism efforts and arrests of suspected criminals. Reports by the Electronic Frontier Foundation (EFF) have led news sources to conclude that, “Immigrant communities are more likely to be the site of biometric data collection than native-born communities because they have less political power to resist it.”[[15]](#footnote-15)

Visitors and immigrants often faced increased, unwarranted scrutiny. We at Access Now have made multiple filings in 2017 responding to requests for comment by the Departments of State regarding their proposal to collect social media identifiers from foreign citizens crossing the United States border. In 2016, when the Department of Homeland Security (DHS) published a request for comment on similar rule changes, Access Now issued a survey requesting public responses to the proposal. More than 2,300 individuals responded with the overwhelming majority of respondents saw the proposal as negative. One respondent explained, “I believe that requesting this information would have a chilling effect on free and open discussion on social media -- discussion that is essential to democracy.”[[16]](#footnote-16)

Surveillance of this sort has a disparate impact on users at risk, including communities of

color, religious groups, LGBTQI communities, and other populations with inordinate rates of impoverishment in the US. Furthermore, when poor communities are targeted with surveillance, they have diminished financial ability and political opportunities to defend their right to privacy.

These invasive practices are not reserved for airports and border crossings. The EFF whitepaper, *From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond,* details extreme surveillance measures employed in policing immigrant day laborer populations in Los Angeles, and indeed across the country. Day laborers, who frequently work for unreported wages far below state minimums, have been the targets of, “[t]he collection of biometrics—such as fingerprints, DNA, and face recognition ready photographs...”

EFF recounts experiences reported by undocumented laborers seeking work in Los Angeles during an unwarranted inspection by the Los Angeles Police Department:

*“They pull out portable fingerprint scanners and tell all the men to line up and have their fingerprints scanned. The men, unsure of their rights but sure that they don’t want to cause trouble, do so… In less than two minutes of scanning each fingerprint, the officer knows whether any of the men has a criminal file or outstanding warrant. Also within that time, the City of Los Angeles has obtained a permanent record of each of the day laborers’ biometric information…”*[[17]](#footnote-17)

The role of private companies in developing, marketing, and supplying tools to directly to law enforcement, as well as indirectly facilitating the growth of social media monitoring and similar commercial and criminal surveillance, should not be overlooked. Silicon Valley, as shorthand for the US internet sector, promotes data collection, retention, and processing on mass scale as the dominant business model.[[18]](#footnote-18) The founders and leaders of internet companies often proceed without regard for the particular impacts their business models can have on vulnerable and marginalized communities. This takes place in part because those very businesses lack representation on staff from potentially affected communities,[[19]](#footnote-19) a longstanding problem noted in the Declaration and Programme of Action of the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance, held in Durban, South Africa, in 2001.[[20]](#footnote-20) The inverse idea -- that the social impact of businesses benefits from such representation -- also appears somewhat true.[[21]](#footnote-21) Unfortunately, the lack of staff diversity, coupled with the “winner takes all” economic model prevalent Silicon Valley companies, means that both the social, cultural, and financial benefits of the internet economy tend to reward those populations already privileged.

**Public assistance predicated on privacy violations**

State-based economic support and government-funded benefits are often exclusively offered to those near or below national poverty thresholds, yet these programs employ massive data collections. “Public-benefits programs, child-welfare systems, and monitoring programs for domestic-abuse offenders all gather large amounts of data on their users, who are disproportionately poor.”[[22]](#footnote-22)

In his book *Overseers of the Poor*, Prof. John Gilliom acknowledges that, “high levels of investigation into the lives of the poor have always been a central part of relief programs” in the United States, “generally designed with little attention to the dignity of the client.”[[23]](#footnote-23) As the United States public-benefits system has transferred gradually to an online infrastructure for enrollment, beneficiaries have been compelled to provide a vast amount of user data. These actions by federal agencies echo long-standing American welfare policy.

Impoverished individuals face financial obstacles in obtaining a reliable internet connection to begin with, as ISPs continue to prioritize wealthy populations with extensions and improvements of already existing service. Once online, impoverished communities face additional challenges around privacy and security.[[24]](#footnote-24) Studies find that, “[m]arginal Internet users’ privacy and surveillance concerns are central to their early encounters with and expectations of the Internet and computers, though formally absent from digital literacy instruction.” Some abandon or avoid the internet entirely over these concerns. Yet many “give up intimate details about themselves in exchange for welfare support.”[[25]](#footnote-25)

Large-scale data collection and retention inherently impinges upon poor communities’ ability to communicate openly and honestly, and to participate in political and social movements. Without extensive reforms, this dynamic is unlikely to change.

**Technology targeting the poor**

Poor communities also face pressures from local authorities, who systematically enforce surveillance systems that unfairly disadvantage low-income neighborhoods. Common among these methods, are urban police departments’ usage of cell-site simulators, or “stingrays.” A stingray is a communications interception technology digitally disguised as a cellular tower, which allows authorities to monitor the activity of an individual’s mobile phone. Last year, investigative news site City Lab found discriminatory use of stingrays, and that, “78 percent of trackable Stingray uses from 2007-14 were found to be in Census blocks where the median household income was lower than the city average.”[[26]](#footnote-26)

Recent attention has been brought to the technology due to complaints from the American Civil Liberties Union and United States senators regarding police departments in Baltimore as well as other American cities with significant populations living under the poverty line. In a joint comment to the FCC, 12 senators stated that they were, “...particularly concerned about allegations that cell site simulators … disrupt cellular service and may interfere with calls for emergency assistance, and that the manner in which cell site simulators are used may disproportionately impact communities of color.”[[27]](#footnote-27)

**Legal gap: no baseline privacy rules in US**

Despite the evident risks of mass surveillance and targeted privacy invasions, the United States lacks any baseline privacy protections for personal data. Rather, a patchwork of state and federal laws imposes a mix of preventive and remedial measures that differ based on the type of data at issue, with evident gaps, including for data processing by internet service providers.

In 2016, the Federal Communication Commission (FCC) proposed and passed "broadband privacy" rules, which put common sense restrictions on how broadband internet service providers were able to use the sensitive information they collect about their customers. The rules empowered individuals to decide whether service providers can share sensitive data with other companies, and provided an opt-out for other uses of their data. The rules also aimed at limiting the threat of malicious online attackers and ensuring notification to users when their data has been breached and exposed. These standards were not only important for people in the U.S. but sent a signal globally that companies handling internet data must respect users’ privacy and safeguard their security.

Access Now supported then-FCC Chairman Wheeler's proposal for several reasons.[[28]](#footnote-28) First, consent gives users control over their data without prohibiting use by providers for reasonable, foreseen purposes. Digital security and data breach notifications standards protect users and fortify user trust. Finally, appropriate privacy rules are not a major burden compared to the significant risks of not applying security and privacy protections. Our full comment is available online.[[29]](#footnote-29)

In March 2017, the Senate used a procedural process called the Congressional Review Act to revoke the rules, and the House of Representatives soon passed a similar bill and sent the issue to the White House.[[30]](#footnote-30) President Trump signed the order, killing the rules before they took effect. After the FCC broadband privacy rules died, several states have stepped up to pass similar rules of their own.[[31]](#footnote-31)

**Conclusion**

We urge the Special Rapporteur to consider these themes during his trip to the United States. In visits with impoverished regions, one should take notice of how lack of network infrastructure affects the economic and political wellbeing of those who live there. With increased pressure and assistance from the international community, there is a far greater chance of improving the oppressive online conditions that exist in the United States today.

We look forward to assisting the Special Rapporteur further in his investigation of the intersections between poverty and human rights.

\*\*\*

*Access Now defends and extends the digital rights of users at risk around the world. By*

*combining innovative policy, user engagement, and direct technical support, we fight for*

*open and secure communications for all.*

*For more information, contact:*

Peter Micek

General Counsel

Access Now

[www.accessnow.org](http://www.accessnow.org/)

Tel: +1-888-414-0100 x709

peter@accessnow.org

1. OHCHR, *Guiding Principles on Extreme Poverty and Human Rights,* [http://www.ohchr.org/Documents/Publications/OHCHR\_ExtremePovertyandHumanRights\_EN.pdf](https://www.ohchr.org/Documents/Publications/OHCHR_ExtremePovertyandHumanRights_EN.pdf) [↑](#footnote-ref-1)
2. United States Census Bureau, *How the Census Bureau Measures Poverty,* <https://www.census.gov/topics/income-poverty/poverty/guidance/poverty-measures.html> (“Following the Office of Management and Budget's (OMB) Statistical Policy Directive 14, the Census Bureau uses a set of money income thresholds that vary by family size and composition to determine who is in poverty. If a family's total income is less than the family's threshold, then that family and every individual in it is considered in poverty”). [↑](#footnote-ref-2)
3. The Center for Public Integrity, *Rich people have access to high-speed Internet; many poor people still don't,*ll<https://www.publicintegrity.org/2016/05/12/19659/rich-people-have-access-high-speed-internet-many-poor-people-still-dont> [↑](#footnote-ref-3)
4. United States Census Bureau, *A Comparison of Rural and Urban America: Household Income and Poverty,* <https://www.census.gov/newsroom/blogs/random-samplings/2016/12/a_comparison_of_rura.html> [↑](#footnote-ref-4)
5. *Ibid.* [↑](#footnote-ref-5)
6. The Center for Public Integrity, *DSL providers save faster internet for wealthier communities,*

   <https://www.publicintegrity.org/2016/10/14/20341/dsl-providers-save-faster-internet-wealthier-communities> [↑](#footnote-ref-6)
7. Federal Communications Commission, *National Broadband Map*, <https://www.broadbandmap.gov/rank/all/state/percent-population/within-nation/speed-download-greater-than-3mbps-upload-greater-than-0.768mbps/ascending> [↑](#footnote-ref-7)
8. See, e.g., AT&T Sponsored Data plan at https://www.att.com/att/sponsoreddata/en/index.html. [↑](#footnote-ref-8)
9. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/35/22, <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22> [↑](#footnote-ref-9)
10. Facebook, *Free Basics Program,* <https://developers.facebook.com/docs/internet-org> [↑](#footnote-ref-10)
11. Alliance for Affordable Internet, *Digging into the Data: Is Zero-Rating Connecting the Unconnected?* <http://a4ai.org/is-zero-rating-really-bringing-people-online> [↑](#footnote-ref-11)
12. Helani Galpaya, LIRNEasia, “Finally, some research on Zero Rated offers and users. And it’s surprising,” 2015:<http://lirneasia.net/2015/10/finally-some-research-on-zero-rated-offers-and-users-and-its-surprising/> [↑](#footnote-ref-12)
13. See Guardian, ‘*Poor internet for poor people': India's activists fight Facebook connection plan*, 15 Jan 2016, at https://www.theguardian.com/world/2016/jan/15/india-net-neutrality-activists-facebook-free-basics. [↑](#footnote-ref-13)
14. See Access Now, *Access Now and EU orgs tell FCC: strengthen, don’t kill, Net Neutrality regs*, at https://www.accessnow.org/netneutralityregs. [↑](#footnote-ref-14)
15. The American Prospect, *Want to Predict the Future of Surveillance? Ask Poor Communities.*, <http://prospect.org/article/want-predict-future-surveillance-ask-poor-communities> [↑](#footnote-ref-15)
16. Access Now, “Thousands object to U.S. plan to collect social media info at border” <https://www.accessnow.org/thousands-object-u-s-government-plan-collect-social-media-information-border/> [↑](#footnote-ref-16)
17. Electronic Frontier Foundation, *From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond,* <https://www.eff.org/document/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond> [↑](#footnote-ref-17)
18. See Washington Post, “How Silicon Valley is Erasing Your Individuality,” https://www.washingtonpost.com/outlook/how-silicon-valley-is-erasing-your-individuality/2017/09/08/a100010a-937c-11e7-aace-04b862b2b3f3\_story.html. [↑](#footnote-ref-18)
19. The Guardian, “Segregated Valley: the ugly truth about Google and diversity in tech,”

    https://www.theguardian.com/technology/2017/aug/07/silicon-valley-google-diversity-black-women-workers. [↑](#footnote-ref-19)
20. Durban Declaration, at para. 144(b), http://www.un.org/WCAR/durban.pdf. [↑](#footnote-ref-20)
21. See, for example, Huffington Post, “Facebook Apologizes To LGBT Community For Controversial Name Change Policy,” at https://www.huffingtonpost.com/2014/10/01/facebook-name-change\_n\_5916336.html. [↑](#footnote-ref-21)
22. The Atlantic, *How Big Data Harms Poor Communities,* <https://www.theatlantic.com/technology/archive/2016/04/how-big-data-harms-poor-communities/477423/> [↑](#footnote-ref-22)
23. John Gilliom, *Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy*. Chicago Series in Law and Society, University of Chicago Press, 2001. See also Micek, Peter. *A Genealogy of Home Visits: Explaining the Relentless Search for Individualized Information Without Individual Suspicion*. 44 U.S.F. L. Rev. 1007 (2009-2010). [↑](#footnote-ref-23)
24. Gangadharan, Seeta Peña (2015). *The downside of digital inclusion: expectations and*

    *experiences of privacy and surveillance among marginal internet users*. New Media and Society. ISSN 1461-4448. Available at <http://eprints.lse.ac.uk/64156/1/Downside_digital_inclusion.pdf>. [↑](#footnote-ref-24)
25. *Ibid.* [↑](#footnote-ref-25)
26. City Lab, *Racial Disparities in Police 'Stingray' Surveillance, Mapped*, <https://www.citylab.com/equity/2016/10/racial-disparities-in-police-stingray-surveillance-mapped/502715/> [↑](#footnote-ref-26)
27. The International Association of Privacy Professionals, *Does Stingray use violate law, target minority communities?*  <https://iapp.org/news/a/does-stingray-use-violate-law-target-minority-communities/> [↑](#footnote-ref-27)
28. Nathan White, Access Now. “On broadband privacy: Working to protect your rights and your data”, 27 May 2016. https://www.accessnow.org/broadband-privacy-working-protect-rights-data. [↑](#footnote-ref-28)
29. Access Now, “Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications

    Services, WC Docket No. 16­106”. 27 March 2016. https://www.accessnow.org/cms/assets/uploads/2016/05/NPRM-PrivacyofBroadbandCustomers-\_-Access-Now.pdf. [↑](#footnote-ref-29)
30. Jim Puzzanghera, L.A. Times. "House sends Trump bill to kill landmark broadband privacy regulations", 28 March 2017, http://www.latimes.com/business/la-fi-fcc-privacy-house-20170328-story.html. [↑](#footnote-ref-30)
31. See NY Times, “Push for Internet Privacy Rules Moves to Statehouses”, <https://www.nytimes.com/2017/03/26/technology/internet-privacy-state-legislation-illinois.html>, and EPIC, “State Broadband Privacy Legislation,” https://epic.org/state-policy/broadband. [↑](#footnote-ref-31)