Surveillance of Muslim and Other Marginalized Communities of Color

Submission to the United Nations Universal Periodic Review of United States of America

Second Cycle
Thirty Sixth Session of the UPR
Human Rights Council
April - May
2020

Submitted by: Justice for Muslims Collective (JMC); Muslim Justice League (MJL)
Contact Name: Dr. Maha Hilal, Co-Director, Justice for Muslims Collective
Contact Phone/Email: (608) 239-3369, maha@justiceformuslims.org
Organization websites/descriptions: Justice for Muslims Collective – JMC (http://www.justiceformuslims.org/); Muslim Justice League – MJL (http://www.muslimjusticeleague.org/)

Justice for Muslims Collective – JMC The mission of Justice for Muslims Collective is to dismantle institutional and structural Islamophobia through raising political consciousness and shifting narratives, community empowerment, organizing and healing, and building alliances across movements with a focus on the greater Washington region.

Muslim Justice League – MJL is a non-profit organization based in Boston, advocating for protection of human and civil rights that are threatened under national security pretexts. MJL was founded after federal announcements Boston would be one of the cities in which the U.S. "countering violent extremism" campaign would be piloted.

I. SUMMARY

1. We are two organizations that work individually and in collaboration on issues of surveillance. Our organizations address surveillance both in a general sense and in particular how it is used as a tactic to criminalize the Muslim community. Surveilling Muslim and other communities of color has resulted in a wide range of consequences including chilling free speech rights, disrupting community cohesion, and criminalizing the community in ways that have lead to detention or worse. Programs surveilling Muslims, has included the heavy use of government informants to entrap vulnerable Muslims, using social media probes to determine evidence of political activism and subsequently identify "suspicious" activities, allowing health and service providers to breach confidentiality on the basis of markers such as support for Muslim causes that might indicate vulnerability to extremism. For the communities that our organizations work with and alongside, surveillance is not simply a matter of an invasion of privacy, it's a direct and targeted attack rooted in the premise of inherent criminality. Moreover, we understand surveillance as part of a larger infrastructure in the War on Terror and one that enables multiple other forms of violence that our communities have continued to experience. As organizations based in the US, we are keenly aware of how post 9/11 policies, rather than protecting the right to be free from surveillance,

have instead been developed to strip our rights further. Moreover, the US' surveillance apparatus has been exported to other countries around the globe, include China which has continued to clamp down on the rights of the Uighurs. The continued use of surveillance by various institutions – local and national in the United States is inherently problematic and the US should work to uphold the protection of the 4th Amendment of the Constitution as well the safeguards in place in the Universal Declaration of Human Rights (UNDHR), the International Covenant on Civil and Political Rights (ICCPR).

II. LEGAL FRAMEWORK

1. The First Amendment to the U.S. Constitution provides that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

2. Article 12 of the Universal Declaration of Human Rights, states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

3. Article 19 of the UNDHR provides that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

4. Article 17(1) of the International Covenant on Civil and Political Rights, provides that: 1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; and 2) Everyone has the right to the protection of the law against such interference or attacks."

5. In a U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018) it asserts that, "Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant."

6. The U.N. General Assembly Resolution on the Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/RES/72/180 (19 December 2017) asserts that States, while countering terrorism are responsible: (i) To safeguard the right to privacy in accordance with international law, in particular international human rights law, and to take measures to ensure that interferences with or restrictions on that right are not arbitrary, are adequately regulated by law and are subject to effective oversight and appropriate redress, including through judicial review or other means; (j) To review their procedures, practices and legislation regarding the surveillance and interception of communications and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law, and to take measures to ensure that interference with the right to

privacy is regulated by law, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that such interference is not arbitrary or unlawful, bearing in mind what is reasonable for the pursuance of legitimate aims;

7. U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018) states that, "Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant,"

8. The Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/71/373 (6 September 2016) 20 states that, surveillance, including both bulk collection of data and targeted attacks on specific individuals or communities, interferes directly with the privacy and security necessary for freedom of opinion and expression, and always requires evaluation under article 19."

III. U.S. COMPLIANCE WITH ITS INTERNATIONAL HUMAN RIGHTS OBLIGATIONS

9. **Countering Violent Extremism at the Federal Level** - In 2015, the Obama administration held the first ever CVE summit. Coincidentally, the Summit happened three days after a hate crime resulting in the murder of three Muslim students in North Carolina. Addressing these students' deaths, President Obama stated that, "no one in the United States of America should ever be targeted because of who they are, what they look like, or how they worship." Despite his statement, CVE has become synonymous with surveilling Muslims and under the Obama administration, 85% of grant money went to programs targeting Muslims under the pretense that Muslims are inherently predisposed to violence. While the CVE grant program was mostly terminated under Trump, CVE programming has continued unabated at the local level in various states, counties, and cities.

10. **Countering Violent Extremism" in Massachusetts** - In 2014, the White House announced that Boston would be the site of a "countering violent extremism" (CVE) pilot program, along with Los Angeles and Minneapolis. CVE is a campaign driven by national security, intelligence and federal law enforcement agencies that purports to steer people off pathways to "radicalization" or "extremism." However, CVE is not supported by sound evidence; it is rooted in discredited theories that "radical" beliefs may predict propensity to commit politically-motivated violence. In practice, CVE falsely legitimizes implicit bias and discrimination against Muslims and political dissidents. CVE programs often recruit non-law enforcement professionals — including doctors, counselors, teachers, imams and others — to engage in soft surveillance, reporting on and referring individuals deemed "vulnerable to extremism" for "interventions" to change their beliefs. CVE thereby interferes with rights to worship, to association, to speech, and to pursue health and education.

1. The Department of Justice (DOJ) and Department of Homeland Security (DHS) have funded a number of CVE programs nationwide and in Massachusetts, some of which are discussed below.
2. In February, 2015, after selecting and convening governmental and non-governmental participants in a number of meetings, the US Attorney's Office for Massachusetts (USAO-MA) — the agency charged with prosecuting federal crimes, including terrorism-related crimes, in Massachusetts — published a framework for CVE in Massachusetts. In Massachusetts, a stated priority of federal prosecutors in deploying the "countering violent extremism" (CVE) campaign has been "Enhanced Communication among Law Enforcement /Mental Health/Social Service Agencies." Specifically, the USAO-MA's CVE Framework states, "In coordination with others, existing methods of communications among law enforcement (local, state and federal), mental health and social service agencies will be assessed so that methods can be enhanced."
3. Additionally, in Massachusetts, the USAO-MA tapped the Massachusetts Executive Office of Health and Human Services ("EOHHS") as a conduit for Department of Justice CVE grant monies, and hosted a session at Suffolk Law School, in Boston, promoting CVE interventions (citing British and German models) for mental health and other social services providers and law enforcement. The routing of Department of Justice CVE monies through EOHHS appears to have been intended to rebrand CVE as a public health — as opposed to law enforcement or surveillance — campaign. And in fact a USAO-MA representative commented to EOHHS staff, in an email released through public records request, that "EOHHS's engagement is key so that this can be framed as a public health issue."
4. Mental health and other health and social services providers are legally permitted, and in some cases mandated, to breach confidentiality where there is imminent risk of harm to a patient/client or another individual. CVE does not propose improvements to existing confidentiality standards; instead CVE recruitment efforts have promoted the idea, without sound empirical support, that vague "concerning behaviors" may predict violence. Explicit guidance about such warning signs is rarely shared publicly, but available guidance cites factors that are extremely broad and common, often particularly common among Muslims (such as "increased activity in a pro-Muslim social group or cause"). Encouraging the mental health sector to be alert to vague and discredited signs of "vulnerability" to "extremism" — in contrast to clear indications of plans for imminent violence — invites use of implicit bias and may also spur invasive or patronizing questioning about clients' and patients' religious or political views.

11. **DHS-funded CVE Surveillance of Somali Diaspora Youth -** In 2017, the Department of Homeland Security (DHS) awarded a CVE grant to a non-profit organization, the Police Initiative, to fund a project called the Youth and Police Initiative Plus (YPIP) which targeted Somali Diaspora youth, age 13-17, in Boston. The Boston Police Department helped plan the project and staffed it with its police officers. YPIP's stated objectives included to "[e]nhance understanding of the violent extremist threat within the Boston Somali community" and to "[b]uild resilience in the Boston Somali community, particularly among youth, to recruitment and participation in violent extremism" through facilitating interactions between Somali Diaspora

youth and Boston police officers. The grant proposal also cited pseudoscientific research claiming to identify factors that cause Somali Diaspora youth to be specially susceptible to "extremism." YPIP engaged local law enforcement in an initiative premised on racist, Islamophobic and xenophobic premises about a community that already faced disproportionate targeting by law enforcement, reinforcing the unjust blanket suspicion Somali Diaspora communities had already experienced.

12. **Social Media Surveillance** - Records obtained by the American Civil Liberties Union of Massachusetts in 2018 demonstrated that the Boston Police Department (BPD) had, from 2014-2016, engaged in social media surveillance of Boston communities and collected posts about religious practices and political activism. BPD opted to be notified of and to collect posts that included search terms such as "Islamic State," "ISIS," "Al-Sham" and even the common Islamic terms "jannah" and "ummah." Posts using these words were classified as "Islamic extremism." BPD's monitoring of these and other terms effectively function to classify political discussion and Muslim religious discussion as suspect and may have contributed to chilled political and religious expression by Muslims in public spaces, including online.

13. **FBI/JTTF Fishing Expeditions -** For many years, agents with the FBI and other component agencies of a Joint Terrorism Task Force (JTTF) have conducted fishing expeditions seeking to interview individuals, especially Muslims, in the absence of any criminal investigation. Often these fishing expeditions result in pressure to act as informants, often through coercive tactics, such as accusations of a false statement made to an agent or a vulnerability in an individual's immigration status. Such FBI/JTTF contact frequently follows international travel to a Muslim-majority country. Documents obtained by The Intercept obtained and publicized documents about interagency collaboration, explaining how "[Customs and Border Protection] assists the FBI in its efforts to target travelers entering the country as potential informants, feeding the [FBI] passenger lists and pulling people aside for lengthy interrogations in order to gather intelligence from them on the FBI's behalf." In addition, according to CUNY CLEAR, the FBI has also been conducting "voluntary interviews," which involves targeting Muslims at work, home, etc. and coercing them to come to their headquarters to ask them questions on foreign policy and personal information that can be used to detect signs of "radicalization."

14. **FBI Entrapment -** Since 9/11, the use of informants in the US has increased ten fold. Before the attacks, there were about 1,500 informants, whereas now there are 15,000 (at least those recorded). FBI informants have sought out vulnerable Muslims and through cultivating relationships with individuals, have provoked those targeted into agreeing to commit acts of violence. Despite the fact that FBI informants have clearly provoked Muslims into committing acts of violence, the US government has always been able to successfully argue in court that the individual targeted, was inherently prone to violence and that the informant was simply moving the process along. This contention has been the default premise with entrapment cases involving Muslims and has reiterated the notion of Muslims' inherent criminality.

15. **FBI Informants** - The use of FBI and other law enforcement informants to conduct widespread surveillance of Muslim spaces of worship, social gathering and service, and political organizing

has had a dramatic and often-discussed (within Muslim communities) chilling impact on myriad forms of public participation. Muslims frequently report that they are hesitate to participate in Muslim Student Associations, to practice their religion in communal spaces (due to a justified perception that they have been coopted for law enforcement surveillance and no longer function to advance their religious purpose) and to state their political views on social media or in other publicly visible fora. Law enforcement treatment of Muslim communities as suspect communities to be broadly monitored — simply due to racist associations of Muslim identity with disloyalty and violence — has effectively suppressed Muslim communities from participating in public life in ways that would advance respect for their communities' rights and well-being, and has severely interfered with Muslims' freedom of association.

16. **Black Identity Extremists** – In 2017, the FBI's intelligence assessment included "Black Identity Extremists," as a domestic terror threat. The anti-Black premise of this label was based on the idea of a consistent theme across killings of the police. Disregarding rampant police brutality against Black people in the US, the obvious intent of this label is to curtail Black activism on state violence and white supremacy in addition to further justifying surveillance against Black activists.

17. **Police surveillance in localities across the United States –** Police departments across the country have been using various surveillance technologies to capture normal citizen activity. In Washington, DC one of the cities where surveillance has continued unabated, the Police have access to technologies not limited to, but including automatic license plate readers, facial recognition software, body cameras, and sting rays. Though these technologies are used under the guise of fighting terrorism, advocates have discovered a much broader use for them including the criminalization of marginalized communities.

18. **Immigration Customs Enforcement (ICE)** – A newly emboldened apparatus for targeting immigrants, ICE has increasingly turned to the tactics of surveillance. Several sources including this one report that ICE agents have not only impersonated identities from police officers to employers to average citizens, they have also gone to Courthouses to surveil and/or captured immigrants' identities. Social media surveillance of immigrants under Trump in particular, have lead to an increase in immigration arrests by 40%. These measures have caused more fear among the immigrant community and have also served to emphasize the idea of immigrants as criminals.

19. **Guantanamo Surveillance** – Attorneys for several Guantanamo prisoners have alleged that they are being surveilled by the Government. Attorneys have detected microphones in meeting rooms with clients in addition to uncovering that the FBI was actively trying to recruit a defense attorney to be an informant on a defense team. Not only has this surveillance caused a serious breach of attorney client privilege, it has also stalled prisoner hearings, and made any semblance of justice impossible.

IV. CONCLUSION

20. The United States has continued to violate domestic and international law concerning

surveillance. Done under the guise of "national security," the surveillance apparatus in the United States has continued to grow with the help of new technologies. The Department of Homeland Security should withdraw explicit and tacit support for the Countering Violent Extremism program because of the model and precedent it has created for localities across the country. Even if addressing white nationalist violence, reviving CVE at the federal level will only serve to creating programming that will inevitably target Muslims. Moreover, the FBI should discontinue it's surveillance and fishing tactics that continue to target Muslim and other communities and which have resulted in the chilling of free speech, disabling communities' freedom of association rights, and the entrapment of vulnerable individuals. In addition, local police forces should abandon the use of surveillance technologies to spy on their citizens and create community task forces to oversee local level surveillance. ICE should cease the use of surveillance technologies to further harass and target already criminalized immigrant communities. Further, Judges overseeing prisoner cases at Guantanamo should ensure that attorney-client privileges are protected and absent government surveillance. Last, a comprehensive Congressional hearing should be held to examine post 9/11 surveillance in the United States with a focus on how Muslims have continued to be targeted under the false premise of protecting national security.