



Universal Periodic Review Consultation with Civil Society
National Security Issues
October 14, 2014

Written Submission of the ACLU on National Security Issues

I. Recruitment of Informants – UPR Recommendation 58¹

The Justice Department will soon be issuing a revision to its Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (“DOJ Guidance”). Among other improvements, the revised DOJ Guidance will reportedly close a loophole that permitted racial profiling in the national security context. It will also reportedly place limits on certain undercover surveillance activities. These would be critical steps forward.

Unfortunately, according to media reports, the FBI interprets the revised Guidance as preserving its authority to target particular religious groups and communities to recruit informants. Preserving such authority would undermine the clarity and force of the revised Guidance. It would diminish the human rights and civil liberties protections afforded by closing the national security loophole. It could also provide a greenlight for the FBI’s continued use of abusive tactics. Accordingly, we urge the Justice Department to ensure that, among other necessary changes,² its revised Guidance unequivocally prohibits the recruiting of informants on the basis of race, religion or national origin.

The FBI has pressured law-abiding American Muslims to become informants against their own communities, often in coercive circumstances. It has targeted immigrants who must rely on the government to process their immigration and citizenship applications in a fair and timely manner.³ It has also used the No-Fly List as leverage to pressure individuals to become informants. FBI agents put this pressure on ACLU clients Abe Mashal, a Marine veteran; Amir Meshal; and Nagib Ali Ghaleb. Each of these Americans spoke to FBI agents to learn why they were suddenly banned from flying and to clear up the errors that led to that decision. Instead of providing that explanation or opportunity, FBI agents offered to help them get off the No-Fly List—but only in exchange for serving as informants in their communities.⁴

¹ Recommendation 58 calls upon the US to “[m]ake fully consistent all domestic anti-terrorism legislation and action with human rights standards.

² The ACLU has also repeatedly urged that a revised DOJ Guidance close loopholes for border integrity, apply to state and local law enforcement agencies that work in partnership with the federal government or receive federal funds, and be made enforceable.

³ See ACLU, *Unleashed and Unaccountable: The FBI’s Unchecked Abuse of Authority* (Sept. 2013), available at <https://www.aclu.org/sites/default/files/assets/unleashed-and-unaccountable-fbi-report.pdf>.

⁴ See ACLU Blog of Rights, *The No-Fly List: Where the FBI Goes Fishing for Informants*, Sept. 27, 2013, <https://www.aclu.org/blog/national-security/no-fly-list-where-fbi-goes-fishing-informants>.

There are also reports that the FBI has targeted Muslim youth to become informants.⁵ While there is no recent and large-scale study of these incidents, some American Muslims have described them as involving intimidation and harassment.⁶

Targeting informants for recruitment based on religion, race or national origin not only amounts to racial profiling, it drives fear of law enforcement and undermines minority communities. Some American Muslims fear that engaging with law enforcement could lead them to be targeted—either to become an informant or, if they refuse, to be retaliated against or even prosecuted. Particularly in this context, recruitment of informants at mosques and community institutions has a chilling impact on political and religious expression. It contributes to anxiety about widespread monitoring and targeting by law enforcement, ultimately undermining community policing.

A revised DOJ Guidance should address human rights concerns raised by the UN Human Rights Committee and UN Committee on the Elimination of Racial Discrimination. Both bodies have urged the US to prohibit racial profiling.⁷ The UN Human Rights Committee has specifically noted the targeting of ethnic minorities and surveillance of Muslims—in the absence of any wrongdoing—by the FBI and New York Police Department.⁸

Recommendations:

- The Justice Department should ensure that any revised DOJ Guidance prohibits the FBI and other law enforcement agencies from recruiting informants on the basis of religion, national origin and race.

II. US Government Watchlisting – UPR Recommendations 58, 188 and 220⁹

In summer 2014, the public learned details about the government’s official watchlisting guidance, which confirmed that the current watchlisting system labels thousands of people, including American citizens, as suspected terrorists based on loose, exception-ridden standards and secret evidence, inevitably ensnaring innocent persons without offering them a meaningful process to challenge errors and clear their names. A bloated and unfair watchlist system

⁵ See Human Rights Watch & Columbia Law School’s Human Rights Institute, *Illusion of Justice: Human Rights Abuses in US Terrorism Prosecutions* 170-171 (July 2014), available at http://www.hrw.org/sites/default/files/reports/usterrorism0714_ForUpload_1_0.pdf.

⁶ *Id.*

⁷ U.N. Human Rights Comm., *Concluding Observations on the Fourth Periodic Report of the United States of America* ¶7 (Apr. 23, 2014), U.N. Doc. CCPR/C/USA/CO/4; U.N. Comm. on the Elimination of Racial Discrimination, *Concluding Observations of the Committee on the Elimination of Racial Discrimination* (Aug. 29, 2014), U.N. Doc. CERD/C/USA/CO/7-9.

⁸ U.N. Human Rights Comm., *Concluding Observations on the Fourth Periodic Report of the United States of America* ¶7 (Apr. 23, 2014), U.N. Doc. CCPR/C/USA/CO/4.

⁹ Recommendation 58 calls upon the US to “[m]ake fully consistent all domestic anti-terrorism legislation and action with human rights standards. Recommendation 188 urges the US to “[a]dopt a set of legislative and administrative measures aimed at ensuring prohibition of the use by state and local authorities of modern technology for excessive and unjustified intervention in citizens’ private life.” Recommendation 220 states: “Smarten security checks so as to take into account the frequent homonymy specific to Moslem names so as to avoid involuntary discrimination against innocent people with such names because of namesakes listed as members of terrorist groups.”

stigmatizes individuals and communities, erodes privacy and has significant human rights impacts.

The FBI's Terrorist Screening Center is the hub of the watchlisting system, and it maintains the master watchlist, or Terrorist Screening Database ("TSDB"). Information from the TSDB flows to various other watchlists and databases, including the No Fly List and the Selectee and Expanded Selectee Lists. Individuals on the No Fly List are prohibited from flying to, from, or over US territory. Individuals on the Selectee and Expanded Selectee Lists are subjected to additional questioning, inspection, and screening before being allowed to board flights to, from, or over US territory.

The standards for inclusion on government watchlists are over-broad and vague. For example, inclusion on the master watchlist requires only reasonable suspicion. Reasonable suspicion, as the government has defined it, requires neither "concrete" nor "irrefutable evidence," and can be based on unverified information or inferences an official draws "in light of his/her experience." This standard is so low that the government's guidelines specifically allow for a single, uncorroborated source of information—including a Facebook or Twitter post—to serve as the basis for placing an individual on the master watchlist. Even information of questionable or doubtful reliability can support "reasonable suspicion"; only information from sources actually "known or determined to be unreliable" is rejected.

Moreover, because the watchlists are not limited to known, actual terrorists, an official can watchlist a person if he or she has reasonable suspicion to believe that the person is a suspected terrorist. In other words, individuals can be watchlisted if they are suspected of being suspected terrorists.

The government's self-mandated watchlisting guidance is also riddled with loopholes and exceptions that permit watchlisting without even a showing of reasonable suspicion. For example, non-citizens can be watchlisted simply for being associated with a watchlisted person even if their relationship with that person is entirely innocuous. Another catch-all exception allows non-citizens to be watchlisted based on fragmentary or uncorroborated information, or information of "suspected reliability."

The result is a watchlisting system that is unreliable and discriminatory. Members of religious, racial, and national origin minority communities and activists regularly report to national and community organizations their experiences of watchlisting based on what appears to be political activism and/or religious observance. Members of these communities are stigmatized, often publicly, and the religious expression of many, especially American Muslims, is chilled.

Recent revelations have confirmed these individual experiences, showing that Dearborn, Michigan—a city with fewer than 100,000 residents that is home to a large concentration of Arab Americans—has more watchlisted individuals than any city in the United States other than New York City. This fact alone presents strong evidence of national origin and religious profiling.

In addition to profiling, watchlists have significant human rights impacts:

- Placement on the No Fly List means an inability to travel by air or sea, while placement on other watchlists can mean invasive screening at airports, denial of a US visa or permission to enter to the United States, and detention and questioning by US or foreign authorities—to say nothing of shame, fear, uncertainty, and denigration as a terrorism suspect.
- Watchlists can separate family members for months or years, isolate individuals from friends and associates, and ruin employment prospects.
- Watchlisting also raises serious privacy concerns. Government officials routinely collect the biometric data of watchlisted individuals, including facial images, iris scans, fingerprints, and DNA strands, and law enforcement has likewise been directed to gather any and all available evidence when encountering watchlisted individuals, including receipts, business cards, health information, and bank statements. This information, in turn, is shared with others. The master watchlist is accessible to at least 22 foreign governments, numerous federal agencies, state and local law enforcement, and even private contractors.
- Compounding this unfairness is the fact that the government fails to provide wrongly or mistakenly watchlisted individuals with an effective mechanism of redress.

Recommendations:

- If the government is to use watchlists, it must ensure that the standards for inclusion are narrow and specific; the evidence being relied upon is accurate and credible; the manner in which the lists are used is appropriately limited and consistent with the presumption of innocence; and the redress and periodic review procedures comport with core constitutional requirements of fairness and due process.

III. Intelligence-Sharing with Foreign Governments – UPR Recommendations 187, 188 and 59¹⁰

Documents leaked by Nobel Prize-nominated whistleblower Edward Snowden have exposed vast global surveillance operations conducted by governments, including the US government. These operations have amassed large quantities of electronic data from billions of people around the world. The US government shares at least some of this data with foreign governments based on both formal agreements and informal arrangements among intelligence agencies. This includes sharing databases, raw data and intelligence reports on the basis of Memoranda of Understanding that are not publicly reported.

For example, the US maintains extensive intelligence sharing arrangements with the United Kingdom, Australia, Canada and New Zealand in a partnership known as the “Five Eyes.”¹¹

¹⁰ Recommendation 187, which the US supports in part, calls on the US to “[g]uarantee the right to privacy and stop spying on its citizens without judicial authorization. Recommendation 59, which the US supports in part, calls on the US to “[l]egislate appropriate regulations to prevent the violations of individual privacy, constant intrusion in and control of cyberspace as well as eavesdropping of communications, by its intelligence and security organizations. For Recommendation 58, *see supra* note 9.

With these countries it shares raw data and intelligence reports, jointly runs operations centers, and utilizes joint intelligence structures.

In addition, the US reportedly shares raw data and intelligence reports with certain countries pursuant to Memoranda of Understanding that are not publicly reported. The US shares raw data and intelligence reports produced by US agencies regarding specific individuals, cases and investigations with both these countries and an unspecified number of other countries. Foreign partners also share data they collect with the US government.

The US also provides support to foreign countries in intelligence collection. As well as sharing raw data and intelligence reports with foreign intelligence agencies, the US also reportedly provides support to Saudi Arabia's Ministry of Defense, arming it with highly advanced surveillance technology.¹²

Despite the extensive nature of its intelligence sharing practices, the United States has failed to disclose what safeguards, if any, it has to ensure that neither US agencies nor foreign governments use collected data to commit human rights abuses, including incommunicado detention and interrogation involving torture or cruel, inhuman and degrading treatment.

Although US law purportedly limits the sharing of intelligence regarding US citizens, in practice safeguards may be limited. In contrast, US guidelines on dissemination of information to foreign governments do not appear to provide any protection to individuals who are not US citizens or permanent residents.¹³ Furthermore, it is unclear what mechanisms, if any, the US has in place to track whether information shared is improperly used to commit abuses or otherwise undermine US interests.

According to reports, the US National Security Agency (NSA) shared the private communications of Americans with an Israeli military-intelligence organization known as Unit 8200 without taking steps to remove identifying information. Moreover, veterans of Unit 8200 have warned that Israel uses information it collects on Palestinians for "political persecution."¹⁴

¹¹ For an analysis of the human rights implications, see Privacy International, *Eyes Wide Open* (Nov. 26, 2013), available at <https://www.privacyinternational.org/resources/reports/eyes-wide-open>.

¹² See Glenn Greenwald and Murtaza Hussain, "The NSA's New Partner in Spying: Saudi Arabia's Brutal State Police," *The Intercept*, July 25, 2014, available at <https://firstlook.org/theintercept/2014/07/25/nsas-new-partner-spying-saudi-arabias-brutal-state-police/>.

¹³ See Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended (2011), sec. 6(b), 8, available at <http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf>; Department of Justice National Security Division & Office of Director of National Intelligence, Semiannual Assessment of Compliance with procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence (August 2013), available at https://www.aclu.org/files/natsec/nsa/semiannual_assessment_of_compliance_with_procedures_and_guidelines_issued_pursuant_to_sect_702_of_fisa.pdf.

¹⁴ See James Bamford, "Israel's N.S.A. Scandal," *New York Times*, Sept. 16, 2014; Letter to Prime Minister Benjamin Netanyahu from veterans of Unit 8200, Sept. 9, 2014, available at <http://www.nytimes.com/interactive/2014/09/12/world/middleeast/13Israeldoc.html>; see also Glenn Greenwald, Laura Poitras and Ewen MacAskill, "NSA Shares raw intelligence including Americans' data with Israel," *The*

US intelligence sharing practices are difficult to document due to their secretive nature, but pose evident risks including torture and ill-treatment. Foreign governments may use information provided by the US government to identify political dissidents, human rights activists, members of religious or ethnic minorities and members of other persecuted or marginalized groups. Foreign governments can use intelligence (both raw data and intelligence reports) shared by the US to track the whereabouts of such individuals and arbitrarily detain them (which could involve secret detention and torture) or extrajudicially kill them. Shared intelligence, in particular raw data, can also lead foreign governments to develop dossiers with which to blackmail such individuals, interrogate them with the use of torture, or prosecute them in unfair trials.

Recommendations:

- All relevant federal agencies should publicly disclose information necessary for assessing US intelligence-sharing practices and the risk they pose to human rights, including—
 - Partner countries:
 - The number and identity of the countries with which the US shares raw data;
 - The number and identity of the countries with which the US shares intelligence on the basis of secret memoranda of understanding; and
 - The number and identity of the countries which the US provides support for surveillance, including provision of surveillance technologies.
 - Standards and procedures for sharing information:
 - The standards and procedures, if any, that limit US sharing of raw data, redacted data, intelligence reports or US person information to countries based on concerns that human rights violations could result;
 - The number and identity of countries with whom the US has suspended intelligence agreements or arrangements, due to concerns that data was being improperly disseminated or used to commit human rights violations;
 - The mechanisms in place, if any, to assess whether raw data or intelligence reports shared with foreign governments are used to commit human rights abuses or otherwise undermine US interests; and
 - The nature and scope of the assurances, if any, the US requires from foreign governments with which it shares raw data or intelligence reports, in relation to its use and possible subsequent dissemination to third countries.
 - Standards and procedures for receiving information:
 - The standards and procedures, if any, that the US employs with regard to data, including raw data and intelligence reports, it receives from foreign countries to ensure that it is not acquired or subsequently used in such a manner that violates human rights of US and non-US citizens or lawful permanent residents; and
 - The standards and procedures, if any, for receiving data from foreign countries that was collected in a manner that does not comply with US or international law.

- Implement policies that prohibit dissemination to a foreign government if there are substantial grounds for believing that sharing that information could lead to the violation of the human rights of individual(s) concerned ; where deficient, enhance mechanisms for auditing whether intelligence information collected and shared by the US government is being used to commit human rights violations or undermine US interests; and ensure that information to, from, or about US persons is not disseminated to foreign governments.

IV. US Drone Strikes – UPR Recommendations 60 and 140¹⁵

Please see Annex I, a letter from the ACLU and other groups to the UN Human Rights Council concerning targeted killings and the use of armed drones.

¹⁵ Recommendation 60 calls on the US to “[t]ake effective legal steps to halt human rights violations by its military forces and private security firms in Afghanistan and other States.” Recommendation 140 calls on the US to “[s]top the war crimes committed by its troops abroad, including the killings of innocent civilians and prosecute those who are responsible.” The US supported both recommendations in part.

Annex I

Letter to the UN Human Rights Council on Targeted Killings and the Use of Armed Drones

To Permanent Representatives of Member and Observer States of the UN Human Rights Council

Geneva, 17 September 2014

Your Excellencies,

The undersigned human rights and civil rights organizations write to share our concerns about state practices of targeted killings and the use of armed drones. We welcome the holding of a panel on the use of armed drones during the 27th session of the United Nations Human Rights Council and urge UN member states to support and take steps to monitor and promote meaningful transparency and legal compliance by states with regard to their targeted killing policies and practices. In particular, we call on states to publicly disclose their targeted killing standards and criteria; ensure that their use or facilitation of lethal force operations abroad comply with international law; enable meaningful oversight and remedies; and ensure effective investigations, tracking and response to civilian harm.

Disclose legal standards and criteria. We are concerned about the lack of transparency in targeted killing operations. While many states affirmed their commitment to transparency at the UN General Assembly in 2013, some states have made only minimal progress in practice. Commitment to the rule of law requires that states disclose the legal constraints on their lethal targeting operations. Greater disclosure of legal and policy standards, and procedural mechanisms, is a prerequisite to informed assessment and debate. We believe this disclosure is an essential first step toward ensuring accountability and redress, and are confident it is possible to improve transparency without putting intelligence sources at risk or endangering national security interests.

Ensure operations comply with international law. States should ensure that their standards and criteria for determining that they can conduct lethal targeting operations are in accordance with international law. The use of force by a state in the territory of another state may be a lawful act of self-defense in response to an armed attack or imminent threat of armed attack. If states permit targeted killings by other states on their territory, they should ensure that such strikes comply with international law. Outside of an armed conflict, where international human rights law applies— including in extraterritorial operations – states can only target individuals who pose an imminent threat to life and lethal force is the last resort; any use of force must be both necessary and proportionate. When states use force as part of hostilities in an armed conflict, there are important legal constraints on targeting operations. For example, civilians may only be deliberately attacked when and for such time as they are directly participating in hostilities, and in cases of doubt as to civilian status, persons must be presumed to be protected against direct attack.

Enable meaningful oversight and the right to a remedy. We are concerned that civilian victims of unlawful attacks are denied the right to access to effective remedies. No state should argue that judicial review of targeted killings is foreclosed. We are also concerned that both domestic and international oversight is inhibited by the lack of transparency. Oversight and judicial review are essential for accountability, and we urge states not to prevent cases alleging serious violations from being heard on their merits, and to fully cooperate with international mechanisms investigating and seeking to provide accountability for wrongful killings.

Ensure effective investigations, tracking and response to civilian harm. Based on a review of a wide range of civilian casualty estimates, we are especially concerned that states may be consistently undercounting and overlooking civilian casualties. A refusal to acknowledge civilian harm is contrary to the rule of law, denies victims the justice they deserve, and compounds anger in impacted communities. These concerns heighten the need to ensure there are effective mechanisms to track and respond to civilian harm.

Many of our concerns are shared by two UN Special Rapporteurs. In 2013-2014 reports, the two UN experts strongly criticise the lack of transparency surrounding these operations. They call on states carrying out these strikes to reveal the number of individuals killed and to investigate all credible allegations of potentially unlawful deaths and injuries. These concerns have also been documented in reports in the last year on targeted killings by Human Rights Watch and Amnesty International.

In light of these concerns, we urge the Human Rights Council, as well as the participants in the HRC Panel on the use of remotely piloted aircrafts or armed drones in counter-terrorism and military operations, to support the following recommendations to states:

- Ensure that any measure employed to counter terrorism, including the use of armed drones, comply with states' obligations under international law, including the Charter of the United Nations, international human rights law and international humanitarian law, as noted in HRC resolution 25/22;
- Ensure transparency on the use of armed drones, to publicly disclose the legal criteria governing their lethal targeting operations, to specify the safeguards in place to ensure compliance with international law, and to conduct prompt, independent and impartial investigations whenever there is credible information of a violation of international law caused by their use;
- Make public the identity and number of individuals killed or injured in targeted killing operations, and the measures in place to prevent civilian casualties and ensure redress when they occur;
- Encourage the Special Rapporteurs on the protection of human rights and fundamental freedoms while countering terrorism and on extrajudicial, summary or arbitrary executions to continue to monitor states' use of armed drones and report back regularly to the Human Rights Council and to the Third Committee of the U.N. General Assembly on states' progress in adopting their recommendations, as well as states' compliance with

international law, and in particular, applicable extraterritorial international human rights obligations, transparency with respect to the legal basis for the use of drones, invocation of self-defence under Article 51 of the Charter of the United Nations, consent to the use of force, and the assessment of civilian casualties, as well as what steps states have taken to ensure meaningful oversight, investigations, and accountability;

- Honor states' own legal obligations with regard to targeted killings taking place within their territory and recognize that states cannot consent to violations of international human rights law or international humanitarian law by foreign states.

Finally, we encourage the Human Rights Council to build upon its resolution 25/22 and adopt a resolution that would reflect the above mentioned points in order to ensure that states meet their international legal obligations. Such a resolution would also help ensure that states uphold their commitment to the Global Counter-Terrorism Strategy approved by the UN General Assembly in 2006, which recognizes that effective counter-terrorism measures and the protection of human rights are “complementary and mutually reinforcing aims.”

We appreciate your attention to our concerns.

Sincerely,

American Civil Liberties Union
Amnesty International
Center for Human Rights & Global Justice, and the Global Justice Clinic, NYU School of Law
Center for Civilians in Conflict
Center for Constitutional Rights
Human Rights Clinic, Columbia Law School
Human Rights First
Human Rights Watch
International Commission of Jurists
Open Society Foundations