INTERNATIONAL HUMAN RIGHTS FUNDERS GROUP

SEMI-ANNUAL CONFERENCE
SAN FRANCISCO
JANUARY 28-29, 2014

World Wide Watching: The Human Rights Implications of National Security Surveillance in the United States and Abroad

Wednesday, January 29, 2014
10:45 am-12:15 pm

Session Organizer and Facilitator:

- Lindsay Ryder, Program Associate, Security & Rights Collaborative of the Proteus Fund

Panelists:

- Maya Berry, Executive Director, Arab American Institute
- Shahid Buttar, Executive Director, Bill of Rights Defense Committee
- Danny O'Brien, International Director, Electronic Frontier Foundation

Sponsor:

- Security & Rights Collaborative of the Proteus Fund

Lindsay Ryder, Program Associate at the Security & Rights Collaborative (SRC) of the Proteus Fund, introduced the session with some background on the U.S. National Security Agency (NSA). The NSA was founded in 1952 and has implemented domestic surveillance programs throughout its existence. Modern surveillance has taken on a new shape based on technological advances, as well as the post-September 11th fear in American society. Responses to NSA activities have increased since September 11th, especially since Edward Snowden, a former NSA contractor, leaked documents revealing the scope of domestic spying in July 2013. On a parallel track, certain communities in America – namely Muslim, Arab, and South Asian communities – have been subject to "targeted" as opposed to "mass" surveillance. They have been profiled and surveilled by law enforcement due to their race, religion, ethnicity and/or national origin. A particularly egregious example is the New York Police Department's surveillance program in which NYC-area Muslims were spied on without warrants or reasonable suspicion. This session hopes to address the rights impacts of these counterterrorism surveillance programs, and draw connections between the mass surveillance and targeted surveillance affecting different communities.

Shahid Buttar, Executive Director of the Bill of Rights Defense Committee, noted two statutes that enable the surveillance dragnet in the U.S.: the Foreign Intelligence Surveillance Act (FISA) and the PATRIOT Act. In legal proceedings, intelligence agencies often cite *Smith v. Maryland*, which found that metadata is not subject to privacy protections under the fourth amendment of the Constitution. However, that case was about a specific individual subject to a targeted investigation, not about mass surveillance of citizens.

Shahid explained that the primary harms of mass surveillance aren't individual but societal rights: surveillance affects freedom of thought. It is difficult for individuals to embrace unpopular thoughts with the government watching, which undercuts democratic tenets. Shahid characterized NSA surveillance as corruption (a secret government agency working with corporations to spy on Americans en masse) and fascism (using executive power to assert social control). The NSA has admitted abuse of its programs, but the possibility of increased abuse is a greater concern. Resistance and opposition cannot flourish when all communications are monitored.

Danny O'Brien, International Director of the Electronic Frontier Foundation (EFF), discussed legal action that EFF has pursued against surveillance in the U.S. EFF has brought cases against telecommunications company AT&T, who were granted retroactive immunity, and against the NSA directly, looking at the threat to freedom of expression and association more broadly than privacy rights. Danny explained that the government uses metadata, rather than targeted spying on terror suspects, to build networks of association. Metadata shows who has communicated with suspected terrorists through multiple degrees of separation, allowing the NSA to sort useful from superfluous information later on.

Danny explained that societal norms in the area of privacy are not well-fixed: many countries have different interpretations of where surveillance fits into rights legislation. Technology has advanced so far that surveillance has become socially acceptable by default. The NSA's surveillance capabilities trickle down abroad and, unlike the nuclear threat, can be deployed by almost any country. For example, the Ethiopian government owns the country's only telecommunications agency, so there are no safeguards against intrusion. The government sends targeted malware to Ethiopian activists working abroad that records activity on the computer, reads email, turns on webcams, and mines contact information to send malware to other computers in the activist's network.

Information technology and the internet allow dissent to spread more quickly, so authoritarian governments often try to intercept communications before they begin. Danny explained that governments use technology to ensure that destabilizing forces don't rise up, especially in African countries.

Maya Berry, Executive Director of the Arab American Institute, then looked at the effects of domestic surveillance on Arab Americans. Citing a report from the Commission on Wartime Relocation and Internment of Civilians (CWRIC), she listed three factors that enabled Japanese internment in the U.S. during World War II: racial prejudice, war hysteria, and failure of political leadership. Maya explained that all three factors are aligned in the U.S. today.

Profiling by the U.S. government has grown to include ethnicity, national origin, and religion. The U.S. Department of Justice is expanding the definition of racial profiling to prohibit ethnic and religious profiling as well, but the national security loophole renders these protections meaningless. Maya offered several examples of institutionalized discrimination against Arab Americans, including the Federal Bureau of Investigation (FBI)'s training materials, the Transportation Security Agency (TSA)'s profiling and SPOT program to identify "suspicious behavior" at airports, and New York City Police

Department (NYPD) surveillance programs. She noted that some colleges have prohibited Muslim student groups from engaging in political conversations on campus.

Maya then discussed the remaining enabling factors: war hysteria and failure of political leadership. She explained that the U.S.'s war on terror enables constant rights violations in pursuit of national security. Arab Americans are subject to increased scrutiny, though only a minority has radical views and an even smaller minority engages in violence. In terms of political leadership, the Arab American Institute grades elected officials to show how they've advocated for or engaged in attacks on Arab Americans and American Muslims. She encouraged the human rights community to engage traditional civil rights advocates when building coalitions around the surveillance issue. Lindsay noted that an Arab American organization supported by SRC succeeded in getting legislation passed to establish NYPD oversight.

Shahid discussed difficulties in undertaking surveillance litigation at the federal level in the U.S. Individuals must establish that they have been monitored in order to have standing in court, and the judiciary has created zones of immunity for executive conduct. Citing a recent speech by U.S. President Barack Obama, Shahid said proposed surveillance reforms would not end bulk collection of data. The U.S. Congress hasn't checked executive overreach, and discussions between the President and Congress have been limited to telephone data, not addressing internet or other electronic surveillance. Shahid pointed to two pieces of legislation with the potential to help: the USA Freedom Act, which would allow companies to release information about mass data requests from the government, and the Surveillance State Repeal Act, which would defund the NSA's bulk collection.

Shahid explained that state and local efforts to fight mass surveillance have found more success in the U.S. The New York City community made progress by breaking down silos, which funders have yet to do. Shahid expressed optimism that shared values like privacy and freedom of thought can unify diverse groups concerned about domestic surveillance, citing movements that included Muslims, African Americans, libertarians, and LGBT people. When adequately funded, such diverse coalitions can achieve results.

Lindsay then turned to opportunities for funders, listing the top 5 grantmaking strategies to address national security surveillance:

- Alliance-building
- Public opinion/media
- Domestic grassroots advocacy
- Litigation
- International advocacy

Danny explained that politicizing surveillance could be dangerous in Washington, D.C., because as soon as reform became one party's issue, it would be opposed by the other. He agreed that alliance-building has been effective, noting one court case that included churches, civil rights, and gun rights advocates. Danny said that many international activists have stopped using technology out of fear of government surveillance, explaining that eliminating methods of peaceful dissent and expression can lead to more

violence. He voiced concern about “privacy nihilism,” in which people surrender to being completely in the open.

The speakers pointed to necessaryandproportionate.org, where a broad international coalition has developed principles showing how surveillance can align with human rights law in the 21st century.

Maya noted that Democrats in the U.S. are eager to appear strong on national security and not to surrender ground to Republicans. She said that politicians will not lead but will follow society’s defined norms. Grassroots advocacy, a coalition of the far left and far right, and public and media opinion are key in recognizing racial, religious, and ethnic profiling as a civil liberties issue, especially among average Americans.

One participant raised the issue of increasing restrictions on foreign funding as another area of concern, noting that donor communications with activists on the ground can put activists at risk as well. Tactical Tech and Frontline Defenders have developed multi-lingual tools showing more secure ways to communicate with human rights activists.