INTERNATIONAL HUMAN RIGHTS FUNDERS GROUP

Surveillance and Profiling: Protecting Human Rights While Confronting "Violent Extremism"

IHRFG-PSFG Federal Policy Briefing, Washington DC
Wednesday, March 30, 2011, 1:30 – 2:45pm

Speakers: Margaret Huang, Executive Director, Rights Working Group; Jameel Jaffer, Director, Center for Democracy, ACLU; Greg Nojeim, Senior Counsel, Center for Democracy and Technology
Moderator: Jameel Jaffer, Director, Center for Democracy, ACLU

Jameel Jaffer opened the session by providing an overview of the state of U.S. government profiling and surveillance initiatives. He noted that there has been a dramatic expansion of government surveillance authority over the past few years, the scope of which is largely unknown by the public. Based on both anecdotal evidence and his experiences with criminal prosecution, Mr. Jaffer noted that the government is using its investigatory powers disproportionately against Arab, Middle Eastern, Muslim and South Asian communities.

Mr. Jaffer continued by offering suggestions for reforms to curtail surveillance injustices. He suggested that the U.S. government change its perspective and strategy for handling this issue, by building coalitions that focus on surveillance issues from the criminal side of the equation, not the national security side.

Greg Nojeim provided an example of a current coalition of the ACLU and the American Library Association with technology corporations such as Microsoft, Google, AT&T, Ebay, and Facebook, companies whose shareholders and customers have a vested interest in protecting privacy.

Mr. Jaffer also highlighted a few areas in need of reform:

- Cell Phone Signals. As it is possible to obtain location information from cell phone signals, there is a need for a strong level of protection for broadcast location information.
- Content of Communications. All content must be protected by a probable cause standard, no matter if opened or how old. Currently, junk mail is the best protected form of communication because if an e-mail is opened, it loses a high level of protection in transit. Furthermore, if an e-mail message is more than 6 months old, then it loses protection because at the time the statue was written it did not account for providers who held e-mails for this duration of time (providers did not have this option at that time).
- New technologies. The FBI is proposing that all new technologies be made wire-tap ready. Affected companies have argued that their products lose attractiveness abroad if the information they contain is easily accessible and monitored by the FBI.

Mr. Jaffer highlighted three major obstacles to using the constitution to challenge surveillance issues:

1) Standing. It is difficult to trace the effects of government policies on ordinary people.
2) Reasonable expectation of privacy test. As technology changes, rights disappear.
3) Third party records doctrine. If information is given to a third party, that information is not constitutionally protected. There is not little information that is not entrusted to a third party (i.e. medical records, school records, information online)

Mr. Jaffer also pointed out a few relevant recent cases addressing surveillance:

1. U.S. vs. Maynard - rejected government claims that federal agents have an unfettered right to install Global Positioning System (GPS) location-tracking devices on anyone's car without a search warrant.
2. Case concerning suspicion-less searching of a laptop at a U.S. border

Margaret Huang shared with participants that the Rights Working Group (RWG) has 293 members who share strategies on backlash faced by certain communities with regard to national security laws. She noted that racial profiling has proven to be successful rallying point for building alliances and community within the large and diverse group. RWG launched a campaign on racial profiling two years ago with two specific policy goals:

1) Enact federal legislation to end racial profiling
2) Change Department of Justice guidance regarding racial profiling. The current definition of racial profiling does not include profiling on the basis of religion or national origin and it only applies to investigatory activities (not surveillance). There is also no mechanism for accountability. RWG would like for this revised definition to be applied to local and state level law enforcement that collaborated with federal enforcement agencies as well.

Question & Answer:

Q: Why do you think enacting federal legislation is best way to address racial profiling?
A: Even if the DOJ guidance were to be fixed, the actions of state and local law enforcement might not be covered. Legislation is the best way to cover all bases. Even at the high levels of the Department of Homeland Security, there is a perception that racial profiling is not a problem.

Q: On the border, are officials allowed to make copies of your information and disseminate that within the U.S. government and to other governments?
A: Yes they are. It is sad, but the safer thing in some situations is not to learn, as that way information cannot be taken away from you. The U.S. government analogizes suitcases and laptops.

Q: What is going on with cyber security? How do we build more public pressure with regard to these issues?
A: When people have their information stolen by bad actors, it is a big problem. One reason for the lack of public pressure with regard to cyber security is that there is no discrete constituency advocating for privacy like there is for other issues, i.e. gay marriage. Everyone benefits from privacy, but because everyone benefits, there are not specific communities that care passionately about these issues. This is similar to the environmental movement thirty years ago.

That movement is a good example for us on how to build a more effective privacy movement. One way to make progress is to work of these issues piece-by-piece and build alliances with unlikely allies.