

ANSWERS TO SENATOR KLOBUCHAR'S QUESTIONS FOR DAVID MEDINE

QUESTIONS FOR THE RECORD

From Senator Amy Klobuchar

“Nominations to the Privacy and Civil Liberties Oversight Board”

April 18, 2012

Questions for all witnesses

Question No. 1: Career Experience

You have all established very impressive careers with experience working in both public service and private legal practice.

- *Can you describe any experiences you have had in your career in balancing civil liberties with national security or other priorities?*
- *How did you go about analyzing such conflicts?*

While in private practice, I supervised two pro bono projects for the bipartisan Constitution Project that presented the opportunity to balance national security and criminal enforcement with civil liberties concerns.

In 2007, American cities had begun to install networks of video cameras in public places to address the increased terrorism threat as well as other concerns about public safety. The cameras could be equipped with technologies such as high resolution and magnification, motion detection, infrared vision, and facial recognition—all linked to a powerful network capable of automated tracking, archiving, and identifying suspect behavior. The cameras could track a person's movements throughout the city, capturing where they went, what they did, and with whom they associated, thus raising concerns about privacy, free speech and association, and equal protection. A report was prepared for the Constitution Project that balanced constitutional rights and values with legitimate law enforcement and anti-terrorism goals, by proposing guidelines for the proper management of video surveillance programs. The guidelines included requiring a clear statement of purpose for the program, conducting a civil liberties impact assessment, restricting tracking of individuals, providing public notice, and establishing safeguards to prevent abuse. This balance would permit use of video surveillance for legitimate purposes while respecting civil liberties values.

Two years later, I assisted the Constitution Project in developing a response to numerous federal agencies' use of over 100 types of labels to designate information, which did not qualify for national security classification, as sensitive but unclassified (SBU) or controlled unclassified information (CUI). There were valid reasons for some documents that did not qualify for classification to, nonetheless, be treated as sensitive with controlled access. However, the SBU or CUI systems lacked any clear standards or accountability with the counterproductive effect of limiting the ability to share such information, which could be put to use in combatting terrorism, with other agencies. The Project's report proposed that a balance be struck between openness in government and protecting sensitive information by creating common government standards and a presumption of openness, increasing access to information by other

federal agencies and the Congress, de-linking CUI identification from responding to FOIA requests, and having these requirements extend beyond terrorist-related information. This approach respected the need to protect certain sensitive information while promoting public accountability and access.

Both of these cases involved government programs with legitimate goals where the methods chosen raised civil liberties concerns. After analyzing the programs, it became clear that changes could be made and guidelines adopted that would permit the programs to proceed consistent with protecting civil liberties.

Question No. 2: Privacy Concerns in the Commercial Arena

Privacy concerns are not just present in the national security context, but also in the commercial arena and with respect to the government's regulation of commerce.

- *Can you talk about how the dynamics or considerations of privacy might be different in commercial contexts as opposed to security contexts?*
- *Specifically, how can industry, including telecommunications firms, and the government work together to improve our approach to privacy issues?*

Whenever information is collected about individuals, privacy concerns can arise, whether it is collection by the government for national security purposes or by private firms for marketing purposes. In the commercial context, there is a tension between companies' wanting as much information as possible about their customers, often to improve their ability to market new products and services, and some customers' discomfort with the collection practices employed. By contrast, in the national security context, the government seeks to collect information with the goal of detecting and thwarting potential attacks on this country and locating and bringing to justice anyone who attempts or carries out such attacks. While protecting our national security is a shared goal, there are legitimate concerns about how much information is collected by the government that could prevent or chill the exercise of civil liberties and also could be subject to abuse.

While these very disparate contexts give rise to privacy concerns, there are common approaches that can be used to address them. One effective approach is "privacy by design." The best, most efficient time to address privacy is during the design process, whether it involves a counterterrorism program or a commercial website that wants to better understand its visitors. It is possible in program design to achieve governmental or commercial goals while respecting privacy concerns. However, it is far harder to make changes to an existing program to address privacy concerns.

Another tool for protecting privacy in the national security and commercial contexts is accountability. The Privacy and Civil Liberties Oversight Board is designed to serve as a check on certain governmental information collection and use practices to make sure they strike the right privacy balance by exercising its oversight authority, including gathering data on what information is being collected and how it is being used. In the commercial context, accountability can be accomplished by providing consumers the opportunity to access information collected about them. The Federal Trade Commission and other government agencies can also use their investigative and enforcement powers to conduct oversight. Self-regulatory organizations can also play an important role.

In addition to working on parallel tracks, there are opportunities for government and the industry to better protect individuals' privacy. Fair information practices (FIPs) have been developed in the private and public spheres. Industry and government could share their approaches to effectively addressing FIPs. For

instance, the Privacy and Civil Liberties Oversight Board is authorized to hold public hearings at which industry and government could collaborate on effective ways to address privacy issues.