Nuala O'Connor
President & CEO
Center for Democracy & Technology
Testimony
Before the
Oakland Privacy Advisory Commission
January 5, 2017

INTRODUCTION

I would like to thank the Privacy Advisory Commission, especially Brian Hofer and Deirdre Mulligan, for extending the invitation to me to be here with you today.

I'm Nuala O'Connor, president and CEO of the Center for Democracy & Technology, nonpartisan, nonprofit advocacy organization dedicated to advancing individual liberty in the digital world. Prior to serving at CDT, I have been the chief privacy officer of both the US Department of Homeland Security and the US Department of Commerce, as well as the global privacy leader at General Electric and VP of Customer Trust at Amazon.

Based on these experiences, I believe that privacy is one of the most compelling challenges for institutions and increasingly one of the values citizens will be scrutinizing in governmental services and actions, particularly in the deployment of new information-gathering technologies.

The boundary between the individual and the state, particularly the increasing intrusion into the private lives of citizens by government agencies through data and internet-enabled surveillance technologies, has been an area of focus for CDT since its founding in 1994, at the dawn of the commercial internet.

Why does this matter? And why do we care, if this surveillance is conducted obviously and in the public square, as opposed to the opaque or clandestine surveillance of communications or in-home activities, which well deserve heightened protections?

This matters because of what our public square means to our democracy. It is the place where we meet, where we gather, where we speak, where we protest. And thus, so closely associated with our freedoms of association and speech, the protection of our public square is essential to our democracy. Ubiquitous surveillance has been shown to have a chilling effect on speech and thought and association.

A recent study from the pew center on internet life showed that after the snowden revelations, over 60% of Americans modified their online search terms or did not engage in internet search - based solely on the assumption that the search might be discovered or monitored. One can extrapolate that actual knowledge, or observed surveillance equipment could have even further

chilling effect on speech or behavior. That chilling effect leads to a loss of ideas, of dialogue, community, and a loss to our democracy.

The proliferation of commonly available surveillance technologies is simply the most recent iteration in the dialogue on governmental authority and individual privacy. It serves all of us - whether concerned about the effective operations of government or about zealously guarding the civil liberties of individuals - to ensure that new technologies are deployed mindfully, taking into account these various equities. This proposal achieves much of the goal of operationalizing and formalizing privacy values, by building it into policy and process. I would recommend further that two additional steps complete a privacy program - one that includes policy, process, people, and technology - first, enhancing internal institutional structures and, second, where possible, reinforcing privacy values in the technology itself by articulating that as a requirement in the acquisition process.

THE PROPOSAL

The Commission and the City are to be commended for the actions taken to consider the privacy impact of new and emerging surveillance technologies, and to implement appropriate processes to ensure these values are taken into account in the acquisition and deployment of new intrusion technologies.

In fact, I would take a step back and observe that while I believe this analysis is merited, in fact, required, in the use of information-gathering technologies by government actors, Oakland and other California municipalities are still on the vanguard of this dialogue - as California so often is - and these ordinances will set a benchmark for other state and local bodies to follow - and we thank you for that. You are ahead of most of your peers across the country and you are paving the way for them.

The proposal provides important checks and balances, as well as necessary independence and perhaps occasional tension where appropriate between the city council and the privacy advisory council.

RECOMMENDATIONS

I. Require standardized impact assessments for the commission's & public's advance comment and review.

The surveillance report and the surveillance use policies should be standardized for ease of citizen review and to streamline the advisory council and the city council's review. Elements of the privacy impact assessment programs at other agencies may be helpful in establishing a sustainable program inside the city entities responsible for the review.

In particular I would emphasize the need - as required in the impact report - for the entities to consider available competing technologies, their costs and relative privacy impacts, and to disclose what other means - including similar devices or different technologies - were considered, and the basis on which those choices were discarded.
This requirement will not only drive decisionmaking by the city entities, but also create incentives for technology offerors to embed privacy values in their products and services.

I would also emphasize the need to articulate how the proposed technology use - in particular any data collection and retention - is narrowly tailored to the task at hand, and how data stored by the government entity will be protected from misuse or attack - whether use by government entities that exceeds initial collection intent or attack by external parties.

As I understand the ordinance, the advisory council bears the brunt of the review and the public report required by section 6 is a report on the prior year.

Absent a showing that confidentiality is necessary, I would argue that a public notice and formal comment period prior to review of of a new surveillance technology by the privacy advisory council, or at least the city council, would strengthen public understanding and awareness prior to the adoption of a new technology.

II. Promote privacy advocates at agencies.

In encouraging the dialogue on privacy and increasing awareness of privacy values among personnel of all job descriptions, including program managers, law enforcement officers, and those responsible for acquisition and deployment of technology, the appointment of internal privacy advocates or champions is one of the most effective ways of ensuring that privacy is discussed at the earliest moments of program design. Certainly by having the Advisory Commission review be a precursor to acquisition is an excellent process. Even more, having internal personnel charged with reviewing the City entity's initiative before even coming to the commission or the council further embeds privacy in the creation and design of government programs and services, while also allowing the people responsible for the outcome of the program to take ownership of embedding privacy values in their own programs while still building for success. Further, while outside review is good and necessary for transparency, inside review is even better as it builds towards sustainable cultures of privacy within the city agencies and entities.

I am mindful of course of organizational sizes and budgets and I would argue this is a function that can be married with existing functions, whether in IT or community relations or ombuds offices. As technology advances this role will likely morph, as it has in the federal service, from a part-time volunteer position to full-time roles with varying expertise, from data to systems to compliance and more. For example, when I began at the Department of Homeland Security, as I like to say, on day three after the creation of the department, with a desk and a pencil, the need to impact a department of almost 200,000 employees looked quite daunting. By creating

not only a headquarters function of privacy professionals, but by encouraging and incubating privacy champions and leaders in each of the almost 40 sub-agencies, that department now has full-time staff on data and privacy in virtually all of those divisions. We did that not by demanding budget and headcount - though those are important - we did it through offering our knowledge as a resource - through education and training - by collaboration.

There is tremendous expertise on this panel alone, and certainly already throughout the city government. A model that could easily be employed, and one that current White House privacy champion Marc Groman has successfully grown - is the creation of an informal council of privacy leaders across the federal agencies - to share information and best practices - leading to greater government efficiency as well as individual privacy protection.

III. Require periodic reports by the privacy advisory commission or another independent third party,

The initial surveillance impact report addresses disparate impact. However, only by additional evaluation after the technology has been deployed, can we truly evaluate whether an unintended disparate impact exists.
I would further require in the annual report an independent assessment of trends in deployment and analysis of potential disparate impact on communities or groups, including those referenced in the city council's findings.

CONCLUSION

The proposal as drafted is a tremendous step forward for accountability and transparency in the deployment of surveillance technologies.

On behalf of the Center for Democracy & Technology, I thank the advisory council for the opportunity to share our thoughts and to lend our support to the creation of not only this policy, but also sustainable structures and processes that will support it.

Thank you.