Seattle Privacy Coalition
Contact@SeattlePrivacy.org
@SeattlePrivacy (twitter)
(206) 310-1218

May 14, 2014

[Elected Official]
City of Seattle
PO Box 34025
Seattle, WA 98124-4025

Dear [Elected Official],

This letter is a response to City Council's request for public input on priorities for the 2015 budget cycle. It introduces the Seattle Privacy Coalition and calls for specific actions to address important and widespread privacy concerns.

We, the undersigned members of the Seattle Privacy Coalition, in partnership with the Seattle Human Rights Commission, ask that you create and implement a formal privacy review process for all new programs and legislation. This process should be documented, repeatable, transparent, defensible, and reviewable by the public.

To support this goal, we call upon the City to fund the following*:

- A privacy impact assessment (PIA) process,
- A citizen's Online Data Privacy advisory board or task force to research and advise on the design of the PIA process,
- A full-time Chief Privacy Officer position to manage the continuing PIA process,
- Staff support for that CPO position.

Why is this important?

Without a consistent, transparent, defensible process for evaluating privacy impacts of new programs and purchases, the City risks wasting taxpayer dollars. For example, the surveillance cameras that the City installed and then removed from Cal Anderson Park, according to the fiscal note with Ordinance 123411, cost the City $145,800 to install, deploy, and then remove.

The City's inability to address privacy concerns also prevents full deployment of the City's already installed mesh network, designed to assist emergency first responders; and has resulted in the installation of 28 unusable surveillance cameras along Seattle waterways from Alki Beach to Alaskan Way to Ballard. The cameras are reportedly disabled, but their fate is in limbo, and they have already cost taxpayers $5 million. The process by which they came to be installed and activated in the first place was unacceptably opaque. Seattle's policies can be updated to reduce such risks.

Finally, Seattle City Light is currently evaluating smart meter technology. According to their public-facing web page, they "are very early in [their] planning process for the transition to digital electric meters," and "will begin installing the meters throughout [their] service area in 2015." This evaluation process is not transparent, and we do not know whether Seattle City Light has been willing or able to avail itself of existing research into privacy-protecting smart meters**.

Seattle's Current Privacy Landscape

We know that the City of Seattle is confronted regularly by lobbyists for data gathering, storage, and analysis equipment companies; including businesses that produce cameras, drones, audio recording devices, and more. These for-profit enterprises have greater resources for articulating the potential benefits of new technologies than privacy advocates have for researching and illuminating the potential risks to privacy that those technologies introduce.

Thanks to the leadership of Councilmembers Harrell and O'Brien, City Council is already gathering information about the potential cost of incorporating a formal privacy review into the City's legislative process.

And consensus appears to be forming on the Council that some action should be taken. In 2010, Councilmember Bagshaw sponsored legislation that resulted in a study of the real and perceived effects of surveillance cameras hastily installed in Cal Anderson Park in 2008, and in the eventual removal of those cameras when they were found by the City Auditor to have been ineffective. In 2013 Councilmember Licata wrote and sponsored legislation that began to address the privacy concerns raised by surveillance equipment. This year, Councilmember Clark has spoken publicly about the need to recognize and address privacy concerns, and Councilmember Sawant has spoken to the need for protecting political speech from inappropriate privacy intrusions.

We at Seattle Privacy Coalition and the Human Rights Commission would like to take the opportunity afforded by the 2015 budget process to press strongly for your support of fully funding and implementing a privacy review process that will serve to protect the people of Seattle as we head ever more decisively into the Information Age.

Seattle can and should set an example for other cities of how to make excellent and effective use of rapidly evolving technology while safeguarding people's liberties. We look forward to helping you make that a reality.

Thank you for the opportunity to provide input into the 2015 budget process.

Yours very sincerely,

Jacob Appelbaum
Tom Bartron
Jan Bultmann
Lee Colleton
Paul English
Beryl Fernandes
Lee Fisher
Mike McCormick
Phil Mocek
David Robinson
Allegra Searle-LeBel
Christopher Sheats
Adam Shostack

Seattle Human Rights Commission

Cc:
Mayor Ed Murray
Councilmember Sally Bagshaw
Councilmember Tim Burgess
Councilmember Sally J. Clark
Councilmember Jean Godden
Councilmember Bruce A. Harrell
Councilmember Nick Licata
Councilmember Mike O'Brien
Councilmember Tom Rasmussen
Councilmember Kshama Sawant

Appendix: Sources and Privacy Risks

*For information about these privacy impact assessments and chief privacy officer positions, please visit this page on the seattleprivacy.org web site: https://www.seattleprivacy.org/sample-code-of-practice-for-privacy-impact-assessments-pias/.

**For information about George Danezis work at Microsoft Research, please visit this page on the Microsoft.com web site: https://research.microsoft.com/en-us/projects/privacy_in_metering/

What are privacy risks?

Privacy has many different meanings, but around the world, it has been effectively brought into the legislative and policy processes. The United Kingdom's Information Commissioner (UKIC) defines privacy this way, borrowing language from the great American privacy law scholar Louis Brandeis:

"Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two main forms, and these can be subject to different types of intrusion:

- Physical privacy – the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.
- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages."

From the same UKIC document, following is a nice summary of privacy risk -- the risk of harm arising through an intrusion into privacy.

"Some of the ways this risk can arise is through personal information being:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept for too long;

- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person that it is about; or
- Not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information. Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance."

Finally, as an example of the type of research and reporting that needs to be done with respect to municipal level privacy protection, we researched the deployment of ShotSpotter**, a system of always-on audio-recording devices intended to recognize the sound of gunfire, in multiple cities in the United States. To see the ShotSpotter Fact Sheet and list of sources, please visit this page on the seattleprivacy.org web site: https://www.seattleprivacy.org/publication/shotspotter-fact-sheet/