4 Safeguards Cities Should Consider When Collecting Constituent Data

Adam Stone | February 22, 2017

Recent moves by the Trump administration make it critical that cities rethink their approach to certain aspects of citizen data, or else risk legal peril.

That's the conclusion reached by the open data advocacy group the Sunlight Foundation in its recently released white paper on protecting data and safeguarding citizens' rights.

The paper lays out 10 municipal guidelines for the collection and management of citizen data. While most of these practices should already be familiar to those concerned with civic data, they have lately taken on a new urgency, said Emily Shaw, an author on the report and a former senior analyst at the Sunlight Foundation.

Of particular concern here is the Jan. 25 Executive Order: Enhancing Public Safety in the Interior of the United States, which effectively makes it a criminal act for cities to fail to comply with certain federal requests for immigration data.

"There are some communities that may have local laws that say the federal government needs to show a warrant if it wants to collect this data," Shaw said. In adhering to its own such statutes, a city could find itself in violation of federal law. If on the other hand

the city ignores its own rules and discloses sensitive data, it could jeopardize citizens whose immigration status is questionable.

Hence the need to reiterate safe and smart data practices, beginning with a fundamental precept that here becomes doubly urgent. Simply put: Don't collect information unless there is a compelling reason to do so.

"Rather than put yourself between a rock and hard place, the better position may be to simply not collect anything you don't need to collect. If you don't need information on someone's immigration status, don't collect that information," Shaw said.

For data junkies — policy chiefs with a passion for numbers-driven decision making — there's always a strong temptation to assume that more is better. The more data points we have, the more complete the picture will be. But as the recent executive order suggests, it may sometimes be possible to know too much. If collecting a resident's immigration information may put that resident at legal risk, some cities may wish to defer.

In practice, this means taking a thoughtful approach to all data-based efforts that touch on citizen information. "You want to clearly map your questions to the purpose of the program that you are collecting information for. Is there a clear mission-related reason for collecting this particular piece of information?" Shaw said. "You don't want to collect something just because it might be useful somewhere down the road. You can just grab a list of questions from a central template, but each time you collect a piece of information, you are potentially putting people at risk."

Rules of the road

The white paper delves into a number of other best practices for cities looking to engage with citizen information.

Where sensitive information is concerned, cities may consider going verbal. Rather than collect formal documentation around a statement, city workers can glean the data in conversation and take appropriate action, without recording an answer that might later put the citizen in jeopardy.

Departments should delete data regularly and often. Policy should generally seek to "minimize, as much as possible, the official retention periods for that data," the report noted.

Be cautious when storing data with third parties. Once data leaves the city's possession and goes to a third party host, U.S. law offers it less protection. "As a result, where departments collect data which reveals citizenship or other vulnerable status, they should avoid hosting or sharing it with a third party vendor," the authors noted. If an outside vendor is needed, consider an international provider whose data may be outside the reach of U.S. laws.

Other significant safeguards include:

1. Encrypt sensitive data and communications: Data encryption practices may include deploying HTTPS across all municipal Web services, requiring full hard disk

encryption on servers and other devices, and using end-to-end encrypted methods of communication rather than those that are not end-to-end-encrypted.

2. Take an inventory of all policies and practices that result in the sharing of information on individuals' citizenship or other sensitive status. Every department should develop a complete inventory of the ways in which it formally and informally provides access to such data. All such policies should be reviewed in light of recent legal changes.

3. Publicly document all policies around data sharing. Governments should tell people what data is available and can be shared with the federal government, so that individuals can opt out of sharing their information where possible.

4. Limit individual employees' discretion on data-sharing. If a government wants to limit data-sharing about sensitive issues to situations where there is a clearly legal requirement for that sharing, it can create policies around this. Such policies could for example explicitly allow employees to resist requests for information made without a court order.

Finally, the foundation encourages municipalities to form oversight bodies to ensure the cities' data protocols are appropriate, legal and well observed. This broad-based body would be a focal point for decision-making on issues related to sensitive citizen data.

Given the complex legal nature of such questions, overlaid with the technical issues surrounding data capture, storage and retrieval, " you need to have some people who have some degree of expertise," Shaw said.

"You need a legal expert, a law enforcement expert, somebody who really knows cybersecurity and somebody who knows how to review policies for accuracy, a detail-oriented person who knows how to read contracts," she said. "The team needs to be able to review government practice, to think about the full range of risks around security and data sharing."

With the executive order of Jan. 25 the nation entered an era in which, perhaps to an unprecedented degree, cities may hold data the very existence of which engenders profound personal peril for a group of citizen.

If cities wish to ensure residents of their continued safety in these circumstances, "they will need both to positively communicate this intention to their residents and also to ensure that they are, in fact, effectively protecting their residents' information," the authors wrote. Sound data management practices will be an integral part of that effort.

http://www.govtech.com/data/4-Safeguards-Cities-Should-Consider-When-Collecting-Constituent-Data.html