Cybersecurity and Immigrant Rights

Megan Ko

ALGA REGIONAL CONFERENCE
PORTLAND, OR

October 3, 2019
Disclaimer: I am

- A performance auditor
- Not an IT, immigrant rights expert
I audited

- Personally identifiable information
- Citizenship information
Two objectives

1. Does the County adhere to best practices for collecting and protecting PII?
2. Are county agencies complying with local law by protecting immigrants’ PII?
I audited

- Personally identifiable information
- Citizenship information
I plan to cover

• Why we did this audit
• How we did this audit
• What we found
• What we recommended
Why do this audit?

- Cybersecurity risk
- Public interest
- Impact (as potential harm avoided)
ICE had access to private arrest data in Seattle despite a sanctuary county law

(CNN) — Immigration and Customs Enforcement agents had access to private information about people arrested in King County, Washington, despite a so-called sanctuary law specifically written to prevent just that, an internal audit found. The audit, released July 9, showed that the issue put ...
I plan to cover

• Why we did this audit
• How we did this audit
• What we found
• What we recommended
Criteria: Best practice, county code

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Recommendations of the National Institute of Standards and Technology

Erika McCallister
Tim Grance
Karen Scarfone

Council adopts guidelines for immigrant and refugee assistance that make King County a “National Model”

February 26, 2018

Summary
Strengthening and clarifying existing County Code

Story
Building on guidelines approved by the Metropolitan King County Council in 2017, the Council today adopted immigration legislation that will make King County a leader in protecting everyone’s safety and civil rights. The ordinance will prevent the use of County funds and resources on federal immigration enforcement and outlines the steps the County will use to protect immigrants and refugees who seek services from the County or are victims/witnesses of crime, while still adhering to federal law.
NIST, GAO definition of PII

Any information about an individual maintained by an agency

(1) any information that can be used to distinguish or trace an individual’s identity; and

(2) any other information that is linked or linkable to an individual

*National Institute for Standards and Technology (2010) citing GAO
PII is anything about an individual

<table>
<thead>
<tr>
<th>NAMES</th>
<th>NUMBERS</th>
<th>CONTACTS</th>
<th>BIOMETRICS</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Bank card</td>
<td>Email address</td>
<td>Fingerprints</td>
<td>Gender</td>
</tr>
<tr>
<td>Full name</td>
<td>Birthdate</td>
<td>Home address</td>
<td>Photographs</td>
<td>Place of birth</td>
</tr>
<tr>
<td>Maiden name</td>
<td>State, federal</td>
<td>Phone number</td>
<td>Retinal scan</td>
<td>Race</td>
</tr>
<tr>
<td>Mother’s</td>
<td>Taxpayer</td>
<td></td>
<td>Voice signature</td>
<td>Religion</td>
</tr>
<tr>
<td>maiden name</td>
<td>identification</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
NIST guidelines

• Identify PII held by the organization
• Minimize use, collection, retention of PII
• Develop controls to safeguard PII
  • Policies and procedures
  • Training
  • Restricting access
Local **immigration** law

Fill in the blanks with your local policy

- Protects PII **of immigrants**
- Prohibits collecting **citizenship** information
- Prevents sharing PII with **civil immigration enforcement**
Scope: Our view of risk

- Citizenship information
- Health records
- Finance records

Recently audited
Scope: Confidentiality impact

- Identifiability
- Quantity
- Sensitivity
- Context
- Obligations
- Location and Access

**Harm:**
Any adverse effects that would be experienced by an individual ... or an organization if ... PII were breached

*NIST 2010*
Citizenship information was harmful

- Identifiability
- Quantity
- Sensitivity
- Context
- Obligations
- Location and Access

High Confidentiality impact level
Evidence: Trust but verify

• Interviews

• Document review
  • Software portfolio
  • User access logs
I plan to cover

• Why we did this audit
• How we did this audit
• What we found
• What we recommended
We found

• Good policy, little practice
• Law enforcement not in compliance
Privacy policy not implemented

• No formal privacy program
• Few designated privacy coordinators
• No inventory of PII
Lack of accountability

Stakeholders focused elsewhere

• Agencies
• Records officers
• IT department
ICE regularly used jail information

In one year:

- 15 ICE users
- Logged in 1,000 times
ICE regularly used sheriff information

In 17 months:

- Received 25 ICE requests
- Gave unredacted files

- Witnesses
- Victims
- Suspects
Agencies not trained on local law

- Training provisions included
- Not widely implemented
- Lack of deadline
I plan to cover

• Why we did this audit
• How we did this audit
• What we found
• What we recommended
Recommendations: Trust but verify

- Clarify roles and responsibilities
- Inventory PII
- Train staff
- Monitor and control access
Some PII is more equal than others

If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds.

—McGeorge Bundy, quoted by NIST 2010

How do we find the diamonds?
Thank you

Full report available online at
KingCounty.gov/Auditor

Questions?
Megan.Ko@KingCounty.gov