CTSC

CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

# Urban Sensor Data Privacy Issues: Findings of the Array of Things (AoT) Privacy Breakout Group

*Von Welch, IU*
*CTSC PI*

*October 27th, 2015*
*trustedci.org*

# Center for Trustworthy Cyberinfrastructure

The goal of CTSC is to provide the NSF community with a coherent understanding of cybersecurity to maximizing trustworthy computational science, and the knowledge to maintain an appropriate cybersecurity program.

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

PITTSBURGH SUPERCOMPUTING CENTER

NCSA

UNIVERSITY of WISCONSIN
UWMILWAUKEE

THE UNIVERSITY of WISCONSIN
MADISON

NSF

## Engagements

LIGO, SciGAP, IceCube, Pegasus, CC-NIE peer review, DKIST, LTERNO, DataONE, SEAD, CyberGIS, HUBzero, Globus, LSST, NEON, U. Utah, PSU, OOI, U. Oklahoma, Gemini, AoT, IBEIS….

## Education, Outreach and Training

Securing Commodity IT in Scientific CI Projects Baseline Controls and Best Practices, Identity Management, Incident Response.

## Leadership

Organized 2013, 2014 & 2015 Cybersecurity Summits for Large Facilities and CI and resulting reports.

Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects.

# Array of Things

Covered by Pete Beckman this morning.

In summary:

- General purpose, extensible, programmable sensors
- Sensors distributed around city
- Sensors gather and process data
    - Allows for situ analysis provided by researchers
- Data fed to city for aggregation
- Distributed by city to data consumers

# AoT Privacy Policy Breakout Group

At AoT Kickoff, Sep 2-4, 2015

Privacy policy critical to acceptance of AoT by citizens.

Breakout group composed of interdisciplinary group of university researchers, city policy makers, and private sector participants.

Providing guidance to project PIs and cities on privacy policy contents.

# Privacy Policy Breakout Group Members

14 Participants included Brenna Berman (City of Chicago Department of Innovation and Technology), Janus Hoeks (Intemo), Bill Howe (U. Washington), Maggie King (U. Chicago), Lee W. Lerner (Georgia Tech), Lindsey-Paige McCloy (City of New York Mayor's Office of Technology and Innovation), Derek Meyer (U. Wisconsin), Michael Ruiz (Georgia Tech), Theo Tryfonas (U. of Bristol), Von Welch (Indiana U.), and Brant Zwiefel (Microsoft).

The opinions expressed in this report represent personal opinions of some, and perhaps not all, members of the breakout group, and should not be interpreted as the position of any organization or project.

CTSC

# Privacy policies need technical and legal input

"Like AUPs, privacy policies can be documents of particular legal significance. Depending on the site or service you offer, to whom you are offering it, what legal entities are involved, the parties' jurisdictional locations, and a host of other factors, your project may want and/or be required to have a privacy policy (or policies), and the policy may be required to meet particular requirements. We strongly encourage you to seek legal assistance (e.g., from your institution's general counsel's office) for assistance in determining the need for, as well as writing and implementing, a privacy policy."

CTSC's Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects

# Stakeholders

Data generators ("sensees")

Data collectors/storers/transporters

In situ sensor researchers

Data distributors (cities)

Data consumers

Will have privacy desires and/or responsibilities.

# Privacy Policy Goals

Sets responsibilities and restrictions on system designers, developers, researchers, and operators.

Informs population ("sensees") of their rights.

PR is a major issue and privacy policy is a key assurance.

# Privacy Policy Challenges Particular to AoT

General-purpose platform & In Situ (vs specific purpose sensors)

Platform will evolve over time with new capabilities

Combination of public and private data

Press currently sensitive to cybersecurity and surveillance

Opt-out infeasible

# Findings

Privacy policy is balance of utility with potential harm to individuals or society: people accept when benefit is clear.

Open access is important. Authentication for access to data not culturally acceptable in U.S. - citizens own data

# Findings (2)

Needs to be code of conduct, with penalities, for in situ researchers. Technical constraints will not be perfect.

Be careful to focus on what instead of how.

Data consumers have privacy - tension with desire to know how data is used by operators.

Understanding trust model between AoT components is key to ensure compliance.

# PP Contents

Easily grasped principles.

Don’t oversell!

- Must be auditable
- Implied promise
- Not only policy doc.

Define data ownership

Allowed data uses

=Terms of Use for data users

Who has physical access to stored data.

Governance - who?

# PP Contents (2)

## Data Categories

Born private or public<br>
Became private or public

Principles for categories and transitions

## Sharing with…

- Partners
- Researchers
- Etc.

Lay out benefits of data collection/sharing to foster acceptance

# Potential Starting Points for PP

Energy metering
Uber
Nest
Twitter
Human subjects
FTC FIPPS
ISO Safe Harbour

Open source Municipal
WiFi polices Healthcare
(Apple watch, Fitbit)
ODB2 in Cars
(Insurance companies)

CTSC

CENTER FOR TRUSTWORTHY SCIENTIFIC CYBERINFRASTRUCTURE

# Thank You

Von Welch
vwelch@iu.edu
trustedci.org

@TrustedCI

We thank the National Science Foundation (grant 1234408) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.