Privacy in the Smart Enough City

Ben Green
Berkman Klein Center for Internet & Society at Harvard
Computer Science Department, Harvard School of Engineering and Applied Sciences

1. What's changed?

"The Failure of Anonymization"
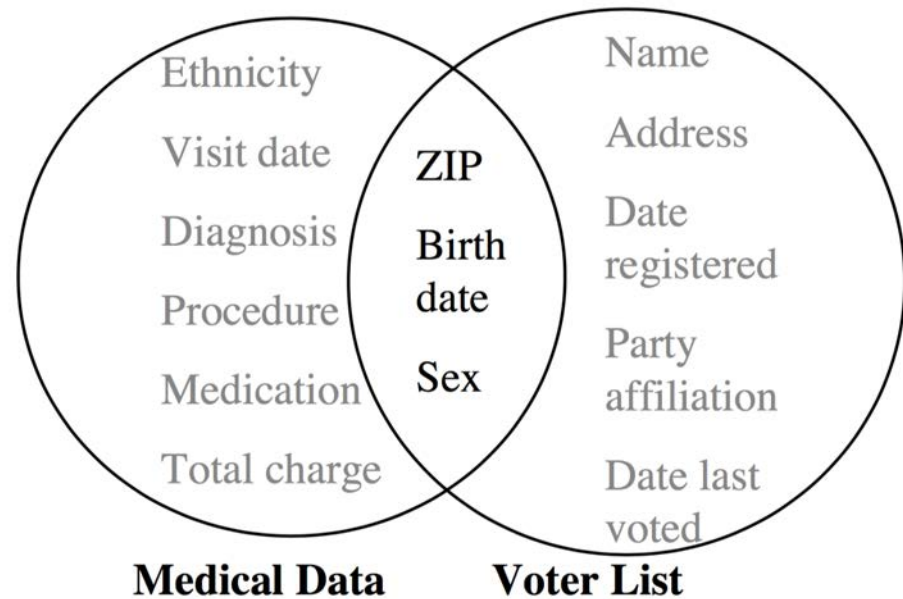
"The Failure of Anonymization"

Mosaic Effect

Figure 1 Linking to re-identify data

birth date alone	12%
birth date and gender	29%
birth date and 5-digit ZIP code	69%
birth date and full postal code	97%

Table 3. Uniqueness of Demographic Fields in Cambridge, Massachusetts, Voter List.
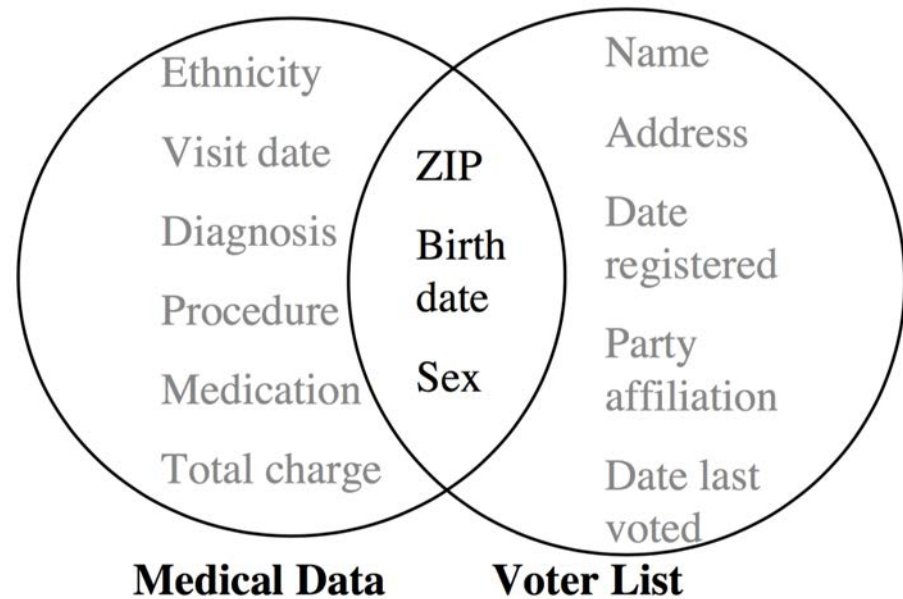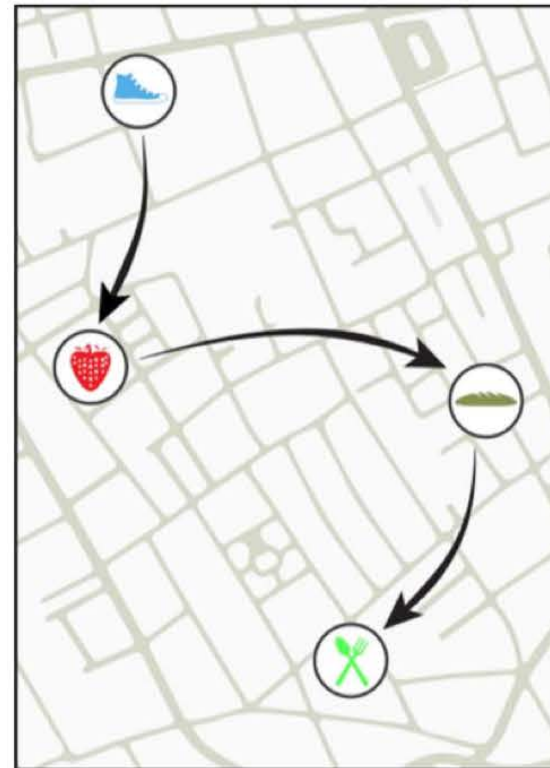
"The Failure of Anonymization"

Mosaic Effect

Figure 1 Linking to re-identify data

birth date alone	12%
birth date and gender	29%
birth date and 5-digit ZIP code	69%
birth date and full postal code	97%

Table 3. Uniqueness of Demographic Fields in Cambridge, Massachusetts, Voter List.

Granular data

4 data-points is sufficient to uniquely identify >90% of people

Municipal data and the limits of de-identification

2013 NYC Taxi Data
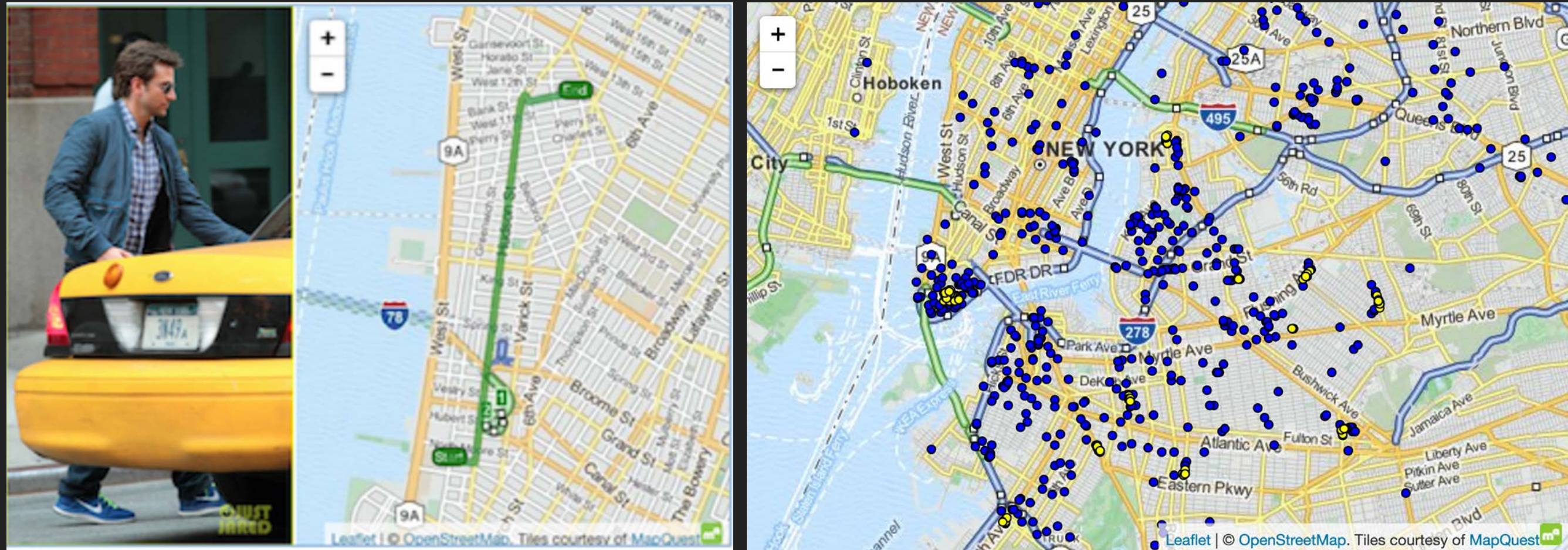
Breach in the armor: public records

▸ Public records laws dictate that certain information must be provided to the public if requested.

▸ There are only very limited exemptions for the sake of privacy.

MA Public Records Law privacy exemption:

• "personnel and medical files or information"

• "materials or data relating to a specifically named individual, the disclosure of which may constitute an unwarranted invasion of personal privacy"

2. How does this implicate cities?

Open data initiatives offer innovation, transparency, and accountability—by releasing more data

Open data initiatives offer innovation, transparency, and accountability—by releasing more data

Domestic Violence

The Switch

Why the names of six people who complained of sexual assault were published online by Dallas police

By Andrea Peterson April 29

Dallas Police Department/Handout via Reuters

Open data initiatives offer innovation, transparency, and accountability—by releasing more data

Domestic Violence

Location Data

The Switch

Why the names of six people who complained of sexual assault were published online by Dallas police

By Andrea Peterson   April 29 ✉

Dallas Police Department/Handout via

Open data initiatives offer innovation, transparency, and accountability—by releasing more data

Domestic Violence
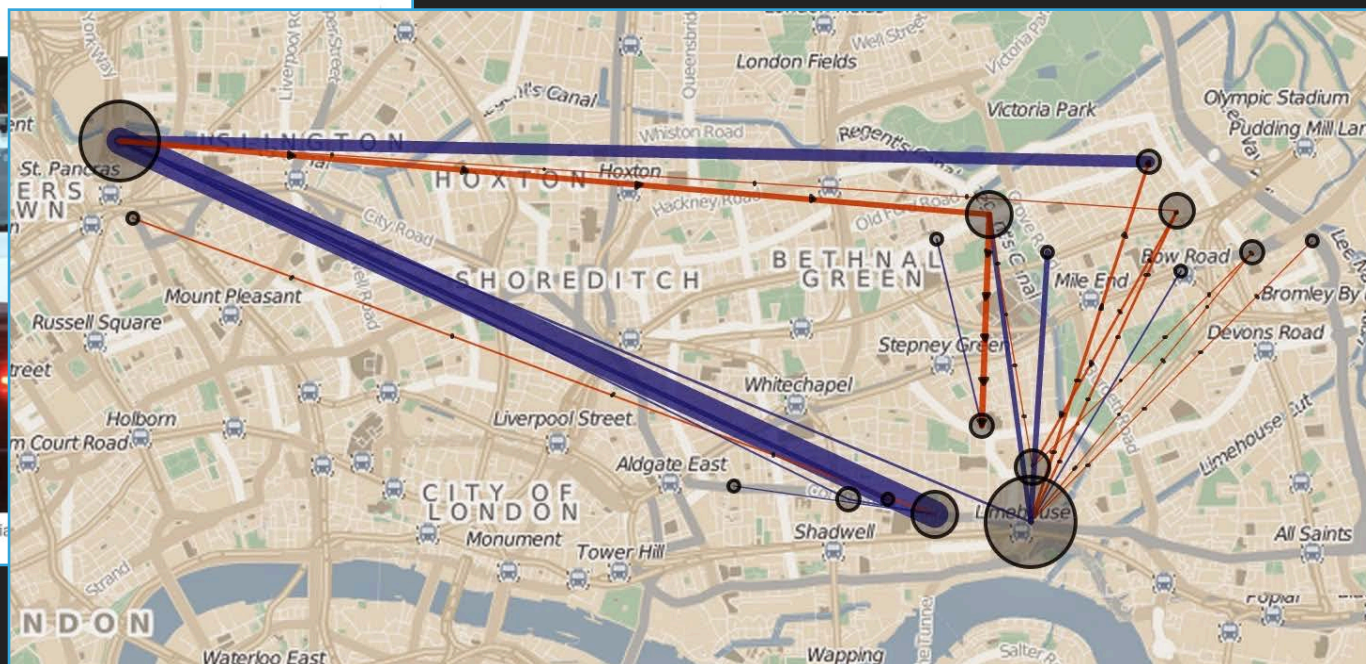
Online vs. Offline Dissemination
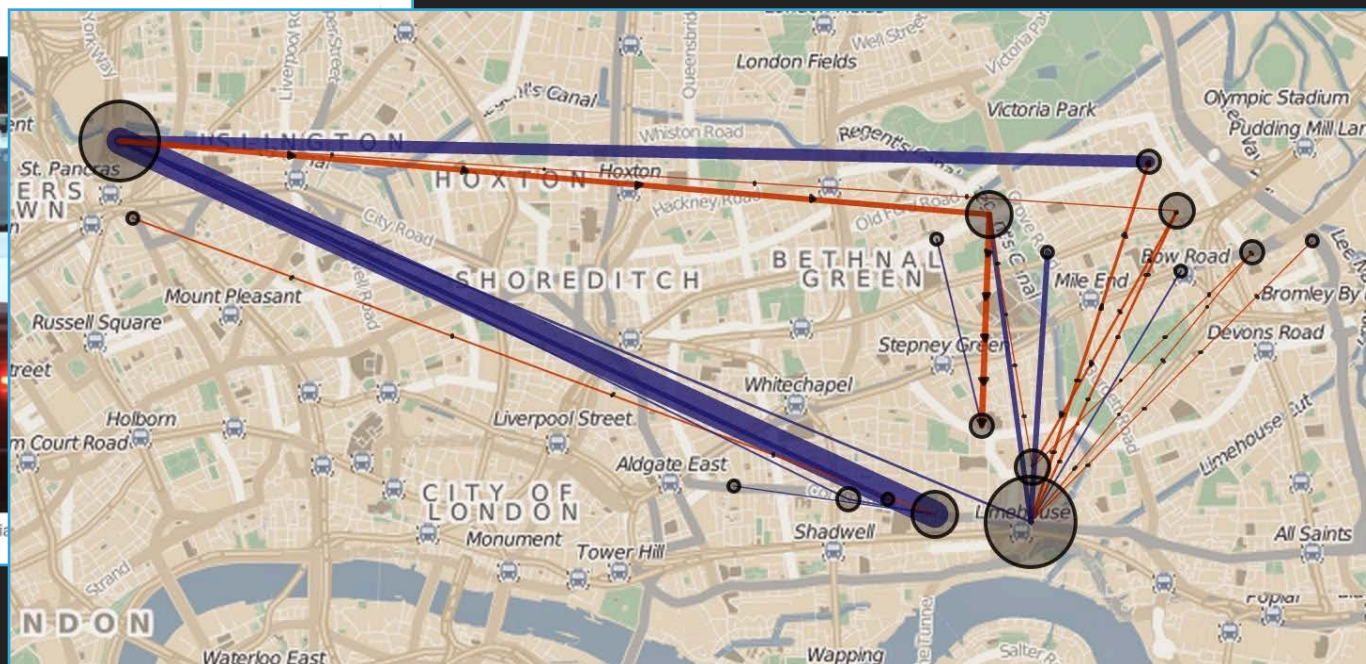
Location Data

The Switch

Why the names of six people who complained of sexual assault were published online by Dallas police

By Andrea Peterson April 29

Dallas Police Department/Handout via

Why the D.C. government just publicly posted every D.C. voter's address online

By Ethan Chiel

Getty Images

Smart cities technologies offer profound operational advances—by collecting more data

Smart cities technologies offer profound operational advances—by collecting more data

Public Private Partnerships

Smart cities technologies offer profound operational advances—by collecting more data

Surveillance Technology

Public Private Partnerships

Smart cities technologies offer profound operational advances—by collecting more data

Surveillance Technology

Public Private Partnerships

Public Engagement

FEATURES   NOV 6, 2013

You Are a Rogue Device

A New Apparatus Capable of Spying on You Has Been Installed Throughout Downtown Seattle. Very Few Citizens Know What It Is, and Officials Don't Want to Talk About It.

by Brendan Kiley and Matt Fikse-Verkerk

Smart cities technologies offer profound operational advances—by collecting more data

Public Private Partnerships

Surveillance Technology

Public Engagement

Proprietary Algorithms

Smart cities technologies offer profound operational advances—by collecting more data

Public Private Partnerships

Surveillance Technology

Opt out?

LOS ANGELES POLICE

Public Engagement

Proprietary Algorithms

FEATURES   NOV 6, 2013

You Are a Rogue Device

A New Apparatus Capable of Spying on You Has Been Installed Throughout Downtown Seattle. Very Few Citizens Know What It Is, and Officials Don't Want to Talk About It.

by Brendan Kiley and Matt Fikse–Verkerk

Get Ready for Super Fast Free Wi-Fi!

#linknyc | www.link.nyc

LinkNYC

3. What should cities do?

The Smart Enough City

The Smart Enough City

‣ False dichotomy: Smart City vs. Dumb City

 ‣ Smart City: Collect as much data as possible to maximize efficiency

 ‣ Dumb City: Collect no data

The Smart Enough City

‣ False dichotomy: Smart City vs. Dumb City

  ‣ Smart City: Collect as much data as possible to maximize efficiency

  ‣ Dumb City: Collect no data

‣ We need not compromise privacy to improve cities

  ‣ Smart Enough City: Collect data based on context and with appropriate policies in place

Data governance requires conscientious privacy management

"if you have a well-resourced, well-functioning privacy program, that program will promote innovation, will actually foster and enable more information sharing and allow agencies to expand to new technologies"

Marc Groman
Former Senior Adviser for Privacy, OMB

Privacy Recommendations for the Smart Enough City

Privacy Recommendations for the Smart Enough City

Open Data

1. Conduct risk-benefit analyses to inform data releases.

2. Take privacy into account at all stages of the data lifecycle.

3. Develop operational structures and processes that codify privacy management.

4. Emphasize public engagement and public priorities.

Privacy Recommendations for the Smart Enough City

Open Data

1. Conduct risk-benefit analyses to inform data releases.

2. Take privacy into account at all stages of the data lifecycle.

3. Develop operational structures and processes that codify privacy management.

4. Emphasize public engagement and public priorities.

Smart Cities

1. Consider privacy before collecting any data.

2. Develop policies that govern access to and control of data.

3. Build support for new initiatives before deployment.

4. Make privacy an essential component of partnerships with private vendors.