Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

Government surveillance

Lorrie Faith Cranor
November 13, 2014

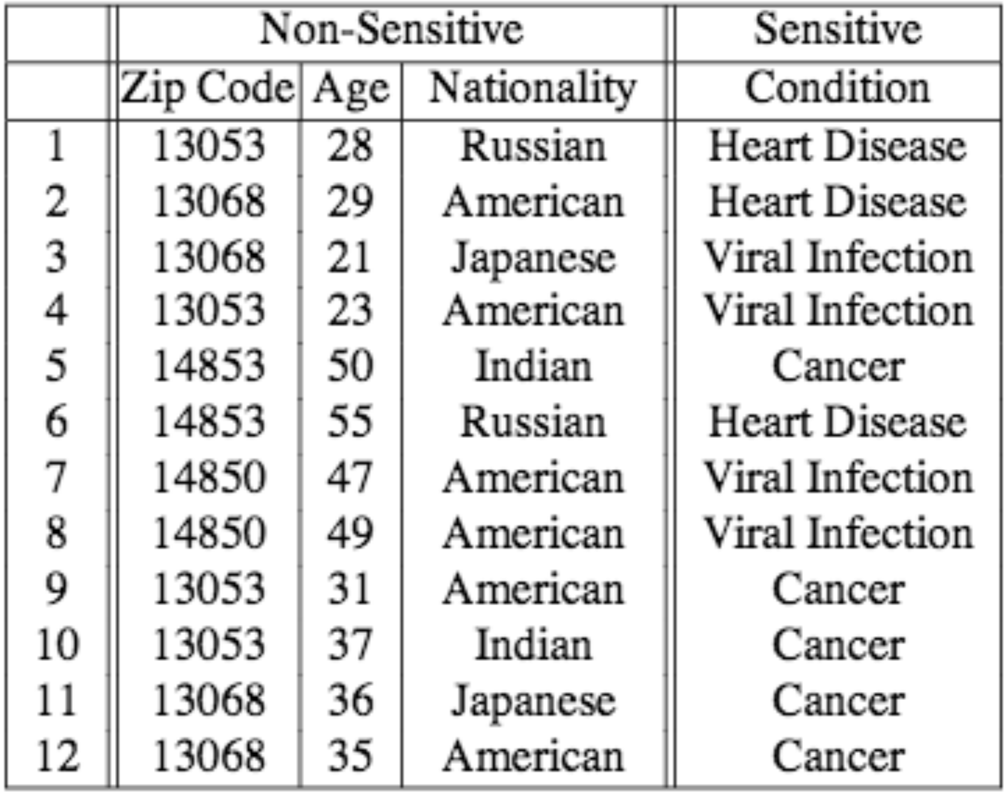
8-533 / 8-733 / 19-608 / 95-818:
Privacy Policy, Law, and Technology

Today's agenda

- Quiz
- Questions/comments about the readings
- Homework questions
- Surveillance
- Videos!

By the end of class you will be able to:

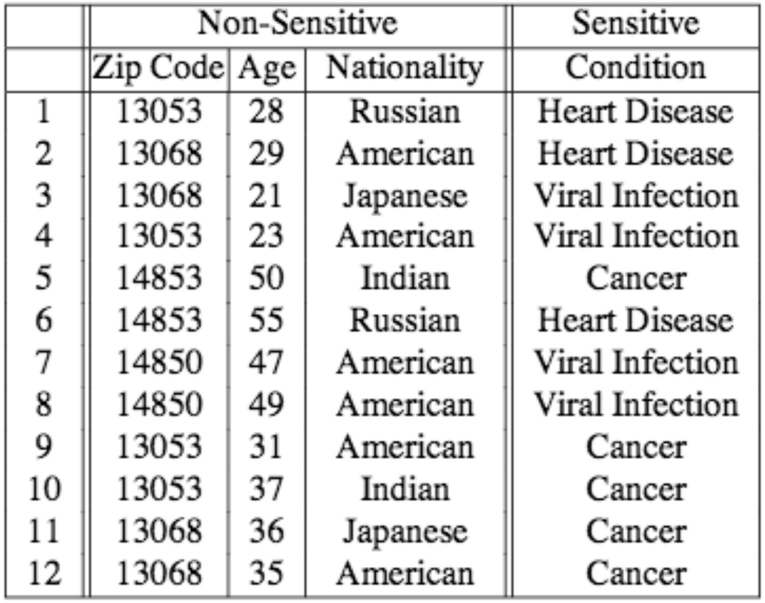
- Be familiar with a variety of US government surveillance programs and the privacy concerns that they raise



	Non-Sensitive			Sensitive
	Zip Code	Age	Nationality	Condition
1	13053	28	Russian	Heart Disease
2	13068	29	American	Heart Disease
3	13068	21	Japanese	Viral Infection
4	13053	23	American	Viral Infection
5	14853	50	Indian	Cancer
6	14853	55	Russian	Heart Disease
7	14850	47	American	Viral Infection
8	14850	49	American	Viral Infection
9	13053	31	American	Cancer
10	13053	37	Indian	Cancer
11	13068	36	Japanese	Cancer
12	13068	35	American	Cancer

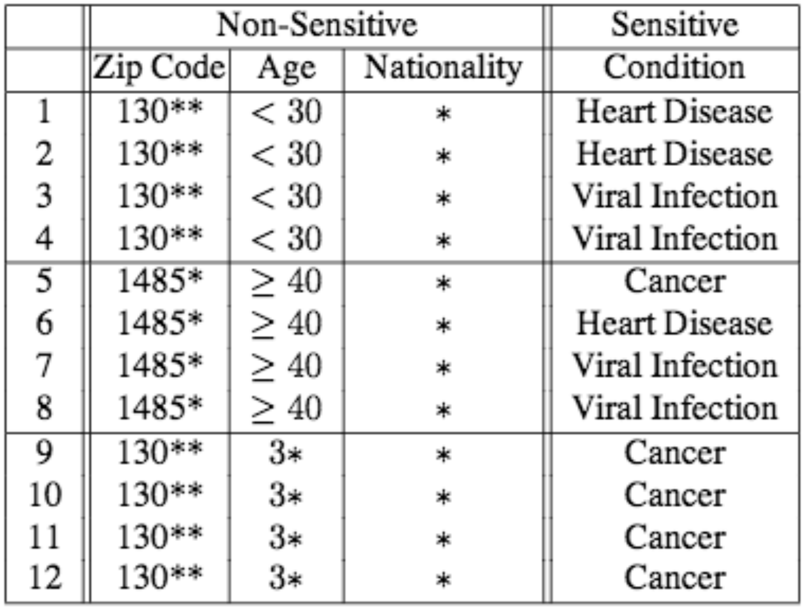
Figure 1. Inpatient Microdata

What value k? what l-diversity?



	Non-Sensitive			Sensitive
	Zip Code	Age	Nationality	Condition
1	13053	28	Russian	Heart Disease
2	13068	29	American	Heart Disease
3	13068	21	Japanese	Viral Infection
4	13053	23	American	Viral Infection
5	14853	50	Indian	Cancer
6	14853	55	Russian	Heart Disease
7	14850	47	American	Viral Infection
8	14850	49	American	Viral Infection
9	13053	31	American	Cancer
10	13053	37	Indian	Cancer
11	13068	36	Japanese	Cancer
12	13068	35	American	Cancer

Figure 1. Inpatient Microdata



	Non-Sensitive			Sensitive
	Zip Code	Age	Nationality	Condition
1	130**	< 30	∗	Heart Disease
2	130**	< 30	∗	Heart Disease
3	130**	< 30	∗	Viral Infection
4	130**	< 30	∗	Viral Infection
5	1485*	≥ 40	∗	Cancer
6	1485*	≥ 40	∗	Heart Disease
7	1485*	≥ 40	∗	Viral Infection
8	1485*	≥ 40	∗	Viral Infection
9	130**	3∗	∗	Cancer
10	130**	3∗	∗	Cancer
11	130**	3∗	∗	Cancer
12	130**	3∗	∗	Cancer

Figure 2. 4-anonymous Inpatient Microdata

Surveillance systems you should know about

- Clipper chip
- Echelon
- TIA
- Carnivore
- CALEA
- MATRIX
- PRISM

Clipper chip

- 1993-1996
- Chipset developed by NSA for encrypting telephone conversations
- Secret “Skipjack” algorithm developed by NSA used “key escrow”
  - Strength of encryption algorithm could not be publicly evaluated
  - Foreign countries would not want their keys escrowed by US gov
- Serious vulnerability pointed out by Matt Blaze
  - Relied on 16-bit hash that could be quickly brute-forced to substitute non-escrowed key, disabling the key escrow

Echelon

- Signals Intelligence (SIGINT) collection and analysis networked operated by Australia, Canada, New Zealand, UK, and US
- Created for military/diplomatic Cold War monitoring, but evolved to monitoring civilians
- Intercepted phone calls, fax, email, etc.
- Uses satellite interception, undersea cables, microwave transmission
- Has list of keywords that are searched for automatically in intercepted messages

Total Information Awareness

- DARPA 2002-2003

Carnivore

- 1997-2005
- FBI system to monitor electronic communication
- Custom packet sniffer to monitor Internet traffic
- Physically located at an ISP or other network
- Required used of custom filters
- Lots of secret details, requires trust that it is legal

CALEA

- Communications Assistance for Law Enforcement Act
- US wiretapping law passed in 1994
- Required telecom carriers and manufacturers to modify their equipment and facilities to allow law-enforcement surveillance

PRISM

- NSA surveillance program operated since 2007
- Collects Internet communications, including encrypted communications
- Many technology companies are participants including Microsoft, Yahoo!, Google, Facebook, YouTube, AOL, Skype, Apple
- Publically revealed by Edward Snowden in 2013

Video

- http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet?language=en

Discussion

- Why do people care?
- Why does this matter?
- What can people do to protect themselves?

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering &
Public Policy