

Your Life, Liberty, and Happiness after the Digital Explosion
BLOWN to BITS
 HAL ABELSON • KEN LEDEEN • HARRY LEWIS

The Authors The Book Blog Excerpts Press Praise Events Buy the Book

"If you want to understand the future before it happens, you'll love this book. If you want to change the future before it happens to you, this book is required reading."
 - Reed Hundt, Former chairman of the Federal Communications Commission

bitsbook.com

How to get over 'getting over' privacy

- **Step 1 – Drop the fig leaf: admit just how broken our legal and technical privacy tools actually are.**

De-identified records

Original Database

Name	Address	ZIP	Birth Date	Sex	Ethnicity
Alyssa P. Hacker	East Campus	02139	05/25/1979	F	White
Ben Bitdiddle	Next House	02139	03/02/1980	M	Black
Joe Law	Baker	02139	07/14/1980	M	Asian
Celine Miles	New House	02139	01/30/1982	F	White

↓ Deidentification

Deidentified Database

ZIP	Birth Date	Sex	Ethnicity
02139	05/25/1979	F	White
02139	03/02/1980	M	Black
02139	07/14/1980	M	Asian
02139	01/30/1982	F	White

The deidentified database looks anonymous, when in fact its subjects can be easily reidentified.

Two separate data bases

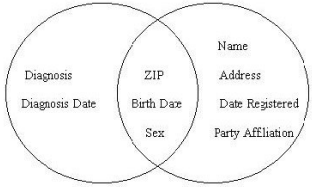
ZIP	Birth Date	Sex	Diagnosis	Diagnosis Date
02139	05/25/1979	F	AIDS	01/21/01
02139	03/02/1980	M	Flu	11/15/00
02139	07/14/1980	M	HIV	03/28/01
02139	01/30/1982	F	Neuroblastoma	07/08/99

De-identified medical research database

Name	Street Address	ZIP	Birth Date	Sex	Date Registered	Party Affiliation
Alyssa P. Hacker	15 Main St.	02139	05/25/1979	F	06/15/97	Democrat
Ben Bitdiddle	68 Broadway	02139	03/02/1980	M	03/03/98	Republican
Joe Law	36 Central Ave.	02139	07/14/1980	M	10/28/80	Democrat
Celine Miles	21 South St.	02139	01/30/1982	F	02/02/00	Republican
...

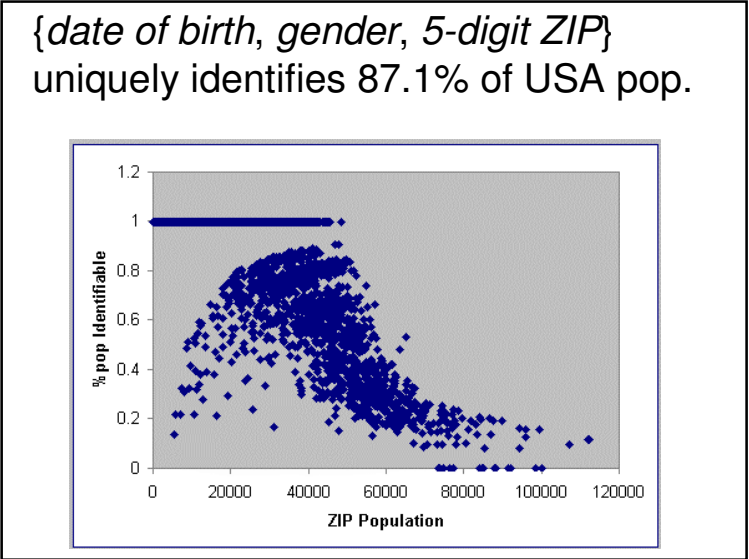
Voter registration list

Re-identification



Find records with the same values in the overlapping fields

Name	Street Address	ZIP	Birth Date	Sex	Diagnosis	Diagnosis Date
Alyssa P. Hacker	15 Main St.	02139	03/25/1979	F	AIDS	01/21/01
Ben Biddie	68 Broadway	02139	03/02/1980	M	Flu	11/15/00
Joe Law	86 Central Ave.	02139	07/14/1980	M	HIV	03/28/01
Celine Miles	21 South St.	02139	01/30/1982	F	Neuroblastoma	07/08/99



Arkansas Juvenile Offender Records

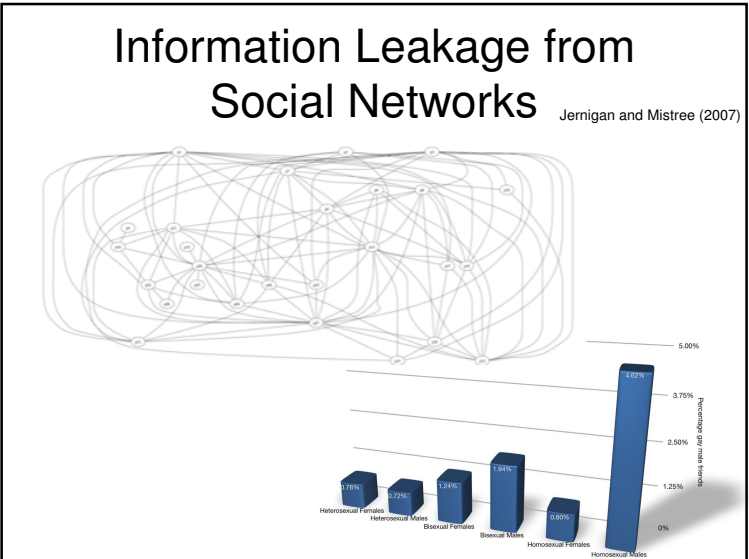
```

01D F77 323RDN94 2 4 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01DWF79 4 9RDN94 2 4 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01DWF81 7 9RDN94 2 4 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01DWM80 523RDN94 2 4 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01DWF82 12 1RDN94 2 4 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01DWM78 2 9RDN94 2 4 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01DWM76 523RDN94 2 2 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01D F7812 5DJ9931020 0 0 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01D M77 317DJ9931026 0 0 0 0 5 36 10398MA 19899899988 98989899988 98941117 0 0 0 OOD
01D M77 725DJ99311 3 0 0 0 0 38 20498MA 1 5 13 20398MC 194 1 5 0 35 OFD
01D M93 519DDN931210 0 0 0 0 9 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01D F89 512DDN931221 0 0 0 0 9 98998999898 98989899988 98989899988 9894 3 4 0 0 OOD
01D F80 327DDN931221 0 0 0 0 9 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01D F81 823DDN931221 0 0 0 0 9 98998999898 98989899988 98989899988 9894 3 4 0 0 OFN
01DWM76 530TD94 1 5 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFDD
01DWM78 522TD94 111 0 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFDD
01D F80 6 4DFS94 125 0 0 0 98998999898 98989899988 98989899988 9894 3 4 0 0 OFF
01D F81 7 3DFS94 125 0 0 0 98998999898 98989899988 98989899988 9894 228 0 0 OFF
01D 9-1999DDN94 3 1 0 0 0 98998999898 98989899988 98989899988 9894 314 0 0 OOD
01D 9-1999DDN94 3 1 0 0 0 98998999898 98989899988 98989899988 9894 314 0 0 OOD
01D F80 721TD94 322 0 0 0 5 36 10398FB 19899899988 98989899988 9894 427 0 0 OFD
01D F80112TD94 322 0 0 0 5 36 10398FB 19899899988 98989899988 9894 427 0 0 OFD
01D F77 616TD94 322 0 0 0 5 36 10398FB 19899899988 98989899988 9894 427 0 0 OFD
01DWM80 223TD94 322 0 0 0 5 36 10398FB 19899899988 98989899988 9894 427 0 0 OFDD
01D F7612TD94 330 0 0 0 5 71 20798MC 1 5 71 2128MC 19899899988 9894 429 200 0 OFD
01DWM77 725TD94 331 0 0 0 5 38 20398FC 2 5 39 2018FB 1 5 32018FC 194 331 0 0 OFDD
  
```

```

01DWF79 4 9RDN94 2 4 0 0
  
```

White, Female,
DOB 1979, April 9



Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Alan Westin, *Privacy and Freedom*, 1967

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others **used by others is ways that affect them.**

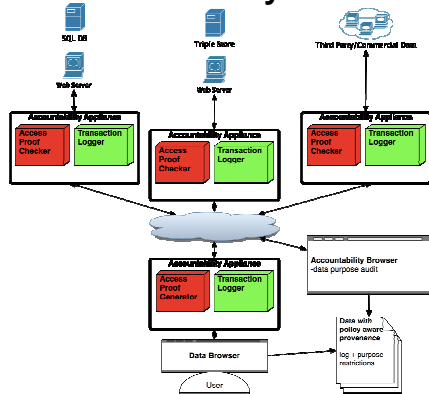
Information accountability

When information has been used, it should to possible to determine what happened, and to pinpoint use that is inappropriate

How to get over 'getting over' privacy

- **Step 1 – Drop the fig leaf: admit just how broken our legal and technical privacy tools actually are.**
- **Step 2 – Build Accountable Systems.**

Accountability architecture



Weitzner, Abelson, Berners-Lee, Feigenbaum, Hendler, Sussman
Information Accountability, 2007

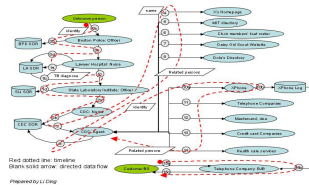
Policy Language for Usage Rules

```
UseOfDataPolicy a deontic:Permission
  deontic:actor ACTOR;
  deontic:action ACTION;
  deontic:constraint { ACTOR a GovEmployee. ACTION
  data DATA. [] a AppropriateUse; actor ACTOR; data DATA }.

{ ACTION data DATA.
  DATA CollectedFor PURPOSE.
  ACTION is PURPOSE. (or has PURPOSE depending on how the
  action hierarchy is defined)
  ACTOR Responsibility RESP,
  PURPOSE is RESP
} => { [] a AppropriateUse; actor ACTOR; data DATA }.
```

Scenario

- In order to prevent an epidemic, CDC contacts everyone whom an unconscious tuberculosis patient could have been in contact with
 - people he works with, his choir, the members of his scout troop, people he has called, who have called him
- CDC gets his phone records from Xphone
- Sometime later Bob Same has phone troubles and calls XPhone to schedule an appt
- The customer service operator sees that CDC had obtained his records and infers that he must have some contagious disease
- So she refuses to schedule a repairman



Event Log

Policy Description

Accountability Reasoning

Information accountability as an alternative to secrecy

- Rules and law should govern how information is used:
"It is illegal to consider health status of applicant or her family in hiring decisions"

⋮

A possible approach to living in an post-private world

- Transparency: You can tell when data flows across “sensitive” boundaries
- Accountability: Data carries with it some notion of “appropriate use”
- Challenge: How do we build an internet architecture that supports transparency and accountability?

⋮