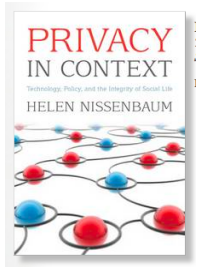
Privacy Panel

Workshop on 2020 Census Data Products

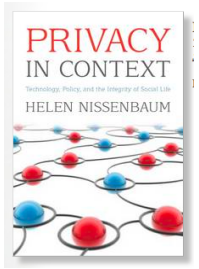
Helen Nissenbaum
Cornell Tech



Privacy as Contextual Integrity

Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>



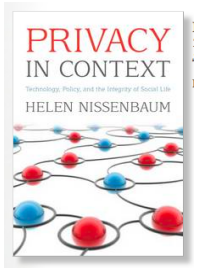
Privacy as Contextual Integrity

Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

Citizens of the US are obliged to reveal gross annual income to the Internal Revenue Service, under conditions of confidentiality except as required by law.

<US Citizens><IRS><gross annual income><required, confidentiality assured per law>



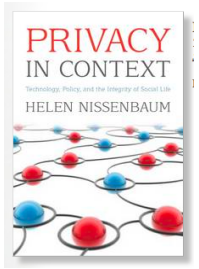
Privacy as Contextual Integrity

Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

Citizens of the US are obliged to reveal gross annual income to the Internal Revenue Service, under conditions of confidentiality except as required by law.
<US Citizens><IRS><gross annual income><required, confidentiality assured per law>

Household residents are required to convey to Census Bureau answers to questions posed in Census form with assurances of strict confidentiality regarding legal ID.
<household residents><US Census Bureau><census info><required, confidentiality of ID>



Privacy as Contextual Integrity

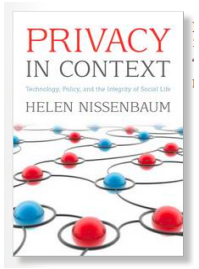
Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

Citizens of the US are obliged to reveal gross annual income to the Internal Revenue Service, under conditions of confidentiality except as required by law.
<US Citizens><IRS><gross annual income><required, confidentiality assured per law>

Household residents are required to convey to Census Bureau answers to questions posed in Census form with assurances of strict confidentiality regarding legal ID.
<household residents><US Census Bureau><census info><required, confidentiality of ID>

Q: Why are these the rules? A: They are legitimate



Privacy as Contextual Integrity

Appropriate flow = follows entrenched norms/rules

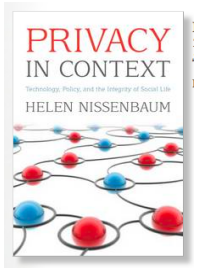
<subject><sender><recipient><information type> <transmission principle>

Legitimate rules
Serve purposes subject to fundamental values

Purposes: Apportionment, redistricting, funding. "Understand nation", useful data for important social sectors (education, commerce, health, etc.)
NOT for administrative, individual level decision making
Values: no harm to individuals through disclosures (privacy) of identified records; maintain trust to secure honest participation and attainment of social purposes

President Taft, circa 1910

"The sole purpose of the census is to secure general statistical information regarding the population and resources of the country, and replies are required from individuals only in order to permit the compilation of such general statistics. The census has nothing to do with taxation, with army or jury service, with the compulsion of school attendance, with the regulation of immigration, or with the enforcement of any national, state, or local law or ordinance, nor can any person be harmed in any way by furnishing the information required. There need be no fear that any disclosure will be made regarding any individual person or his affairs. For the due protection of the rights and interests of the persons furnishing information, every employee of the Census Bureau is prohibited, under heavy penalty, from disclosing any information which may thus come to his knowledge."



Privacy as Contextual Integrity

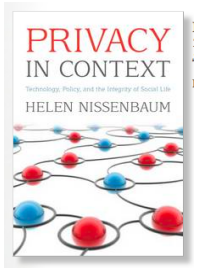
Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

1790: 5 questions, posted in a public place (Age: <16 and >16)

1800s: Age range, increasingly fine grained

1910: 32 questions (Age)



Privacy as Contextual Integrity

Appropriate flow = follows entrenched norms/rules

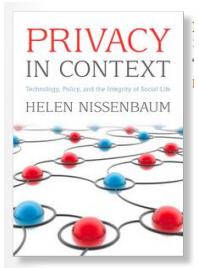
<subject><sender><recipient><information type> <transmission principle>

1790: 5 questions, posted in a public place (Age: <16 and >16)

1800s: Age range, increasingly fine grained

1910: 32 questions (Age)

Note: as # of questions grew, and questions grew more granular, worry grew, direct answers were no longer posted, a confidentiality commitment grew



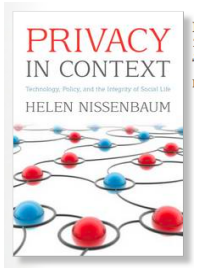
Privacy as Contextual Integrity

Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

Shameful moments

- WWI Census Bureau provided information to DoJ and military about draft age men
- 1920s Toledo Census office provided citizenship information for Dept of Labor deportation cases
- WW2 CB gave information about Japanese Americans to US War Department (?)



Privacy as Contextual Integrity

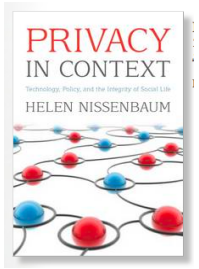
Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

Shameful moments

- WWI Census Bureau provided information to DoJ and military about draft age men
- 1920s Toledo Census office provided citizenship information for Dept of Labor deportation cases
- WW2 CB gave information about Japanese Americans to US War Department

Broke commitment
Undermined fundamental values: privacy, security, trust



Privacy as Contextual Integrity

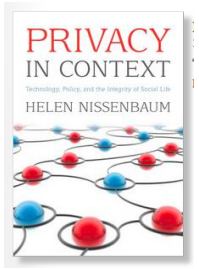
Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

Shameful moments

Upshot: Title 13 (with apology to complexity of detail)

Broke commitment
Undermined fundamental values: privacy, security, trust



Privacy as Contextual Integrity

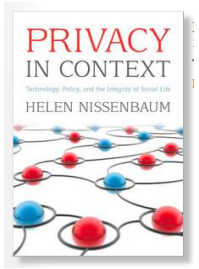
Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

The present time:

Using aggregate products from 2010 Census,
It's possible to recreate individual records and reattach to legal identifiers!!!

Compare,
"We only publish statistics. Our policies and statistical safeguards help us ensure the confidentiality of your information." (From census.gov)



Privacy as Contextual Integrity

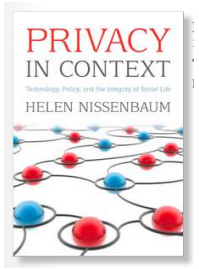
Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

The solution space?

Doing nothing?
… is not status quo

Q: Why are these the rules? A: Status quo and meet legitimacy standards
Q: What makes rules legitimate? A: Serve contextual goals and values



Privacy as Contextual Integrity

Appropriate flow = follows entrenched norms/rules

<subject><sender><recipient><information type> <transmission principle>

The solution space?

Limit who gets what

Slash # questions

Decrease granularity

Impose conditions

Differential Privacy