Understanding privacy through the lens of contextual integrity

Helen Nissenbaum, Cornell Tech

Remarks prepared for NCVHS: Privacy, Confidentiality, and Security Perspectives on Data Collection and Use during the COVID-19 Public Health Emergency

2020 June 19

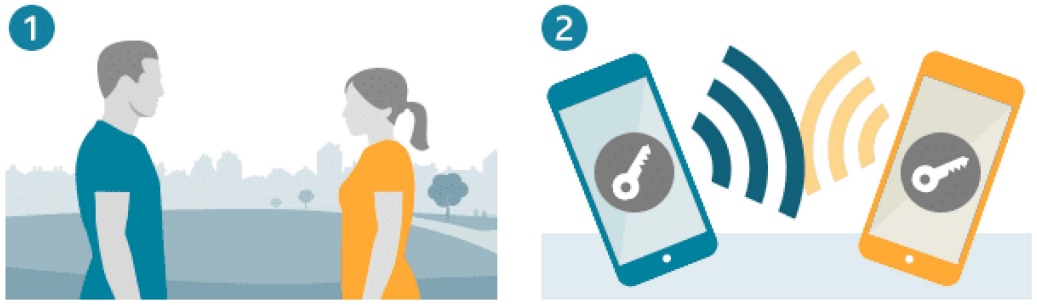
An approach to thinking about tech-assisted health surveillance

Not a solution.

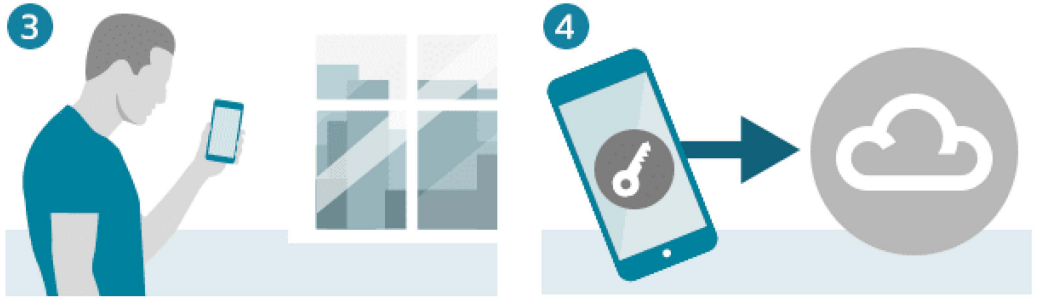
Mobile phone enabled contact tracing merely, an illustration

or, how to avoid Trojan horses

What Apple and Google have proposed



When A and B meet, their phones exchange a key code



When A becomes infected, he updates his status in the app and gives his consent to share his key with the database

B's phone regularly downloads the database to check for matching codes. It alerts her that somebody she has been near has tested positive

Source: Apple/Google

BBC

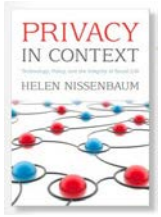
Wouldn't we like to know:

- The connection between key code and phone IDs, and who knows this.
- How A's (public health authority) app is updated with COVID+ status
- Where the database sits, and what analytics can be performed by whom
- What/whose models inform the decision that B has been near enough to be alerted?
- Whether database is updated.
- Whose models can be updated ("learn") if B becomes COVID+ (or if not)
- Where processing is done: Google/Apple? App developer? Public health authorities? Governments?

Not all questions are about privacy!

Privacy commonly:

- Right to control information about ourselves
- Right to have information about ourselves withheld (secrecy)
- Above, but regarding private/sensitive information, not public



Theory of Contextual Integrity

Privacy as "**Appropriate** Flow"

Flow conforms with

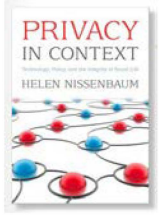
Legitimate contextual informational norms

Key terms

Contexts: social domains {healthcare, education, politics…}

Informational norms: {actors <Su,Se,Re>, i-types, transmission principles}

Legitimate informational norms



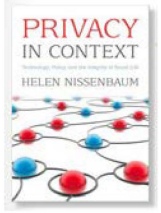
Theory of Contextual Integrity

Requires flow to conform with

Legitimate contextual informational norms

1. Contexts: social domains {healthcare, education, politics…}
2. Informational norms: {actors <Su,Se,Re>, i-types, transmission principles}
3. **Legitimate** informational norms?

- Interests;
- Societal values;
- Contextual ends, purposes, values



Theory of Contextual Integrity

?Does *flow conform with*

Legitimate contextual informational norms

1. Map flows in terms of 5 parameters {Su, Se, Re, i-types, TPs}
2. Compare with entrenched I-norms (This is an empirical question.)
3. **Assess Legitimacy** of flow vs. norm

- Interests
- Societal values
- Contextual ends, purposes, values

Received: 31 August 2019 | Revised: 23 December 2019 | Accepted: 18 February 2020

DOI: 10.1002/asi.24353

Check for updates

RESEARCH ARTICLE

JASIST WILEY

Disaster privacy/privacy disaster

Madelyn R. Sanfilippo[1] | **Yan Shvartzshnaider**[1,2] | **Irwin Reyes**[3] | **Helen Nissenbaum**[4,5] | **Serge Egelman**[6]

[1]Center for Information Technology Policy, Princeton University, Princeton, New Jersey

[2]Courant Institute of Mathematical Sciences, New York University, New York, New York

[3]International Computer Science Institute, University of California, Berkeley, California

[4]Digital Life Initiative, Cornell Tech, New York, New York

[5]Information Science Department, Cornell University, Ithaca, New York

[6]Department of Electrical Engineering

Abstract

Privacy expectations during disasters differ significantly from nonemergency situations. This paper explores the actual privacy practices of popular disaster apps, highlighting location information flows. Our empirical study compares content analysis of privacy policies and government agency policies, structured by the contextual integrity framework, with static and dynamic app analysis documenting the personal data sent by 15 apps. We identify substantive gaps between regulation and guidance, privacy policies, and information flows, resulting from ambiguities and exploitation of exemptions. Results also indicate gaps between governance and practice, including the following: (a) Many apps ignore self-defined policies; (b) while some policies state they "might"

App	Location Permissions				User options		
					Location-services	In versus out of app	Other location
MyRadar Weather Radar							
Red Cross Hurricane	√	√					√
Red Cross Emergency	√	√					√
My Earthquake Alerts							
My Hurricane Tracker							
Storm Tracker Weather Radar							
NOAA UHD Radar & NWS Alerts							
Storm Tracker: NOAA Weather Radar & Live GPS Maps							
The Weather Channel Live Maps	√	√			√	√	
Weather Underground: Forecasts	√	√			√	√	
FEMA							
Dark Sky							
National Weather Service No Ad							
NOAA Weather Radar Live & Alerts							
Global Storms	√	√	√		√	√	

Studied data flows for 15 Disaster apps

Static analysis: code + permissions

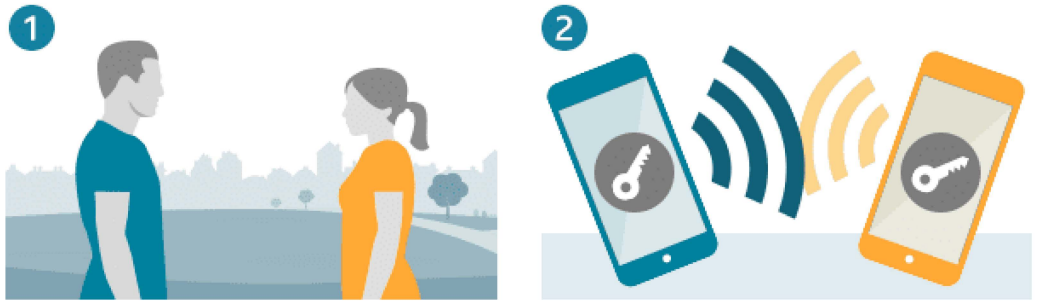
Dynamic analysis: mapped information flows in terms of 5 Parameters of contextual informational norms, utizing instrumented Android OS (*AppCensus*)

Measure flows against norms: Utilized law & regulatory guidance; endogenous privacy policies; surveyed user comments

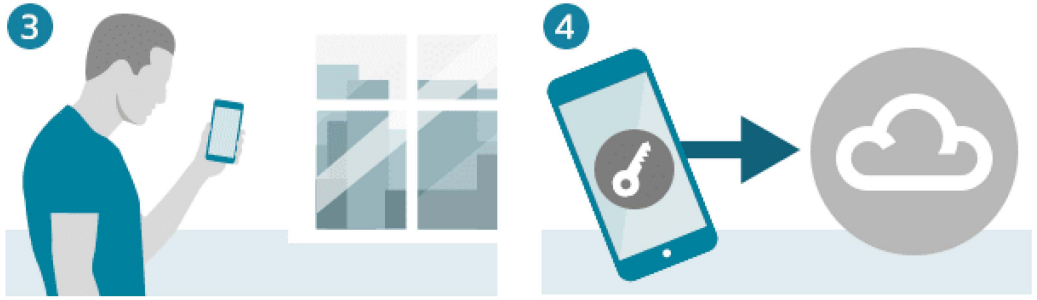
Results: GAPS BETWEEN GOVERNANCE AND PRACTICE

2. Compliant with Exogenous Governance	1. Compliant
My Hurricane Tracker My Earthquake Alerts MyRadar Weather Radar Storm Tracker Weather Radar The Weather Channel Live Maps Weather Underground: Forecasts	FEMA National Weather Service No Ad NOAA UHD Radar & NWS Alerts
4. Non-compliant	**3. Compliant with Endogenous Governance**
Red Cross Emergency Red Cross Hurricane	Dark Sky Global Storms NOAA Weather Radar Live & Alerts Storm Tracker: NOAA Weather Radar & Live GPS Maps

What Apple and Google have proposed



When A and B meet, their phones exchange a key code



When A becomes infected, he updates his status in the app and gives his consent to share his key with the database

B's phone regularly downloads the database to check for matching codes. It alerts her that somebody she has been near has tested positive

Source: Apple/Google

BBC

Wouldn't we like to know:

- The connection between key code and phone IDs, and who knows this.
- How A's (public health authority) app is updated with COVID+ status
- Where the database sits, and what analytics can be performed by whom
- What/whose models inform the decision that B has been near enough to be alerted?
- Whether database is updated.
- Whose models can be updated ("learn") if B becomes COVID+ (or if not)
- Where processing is done: Google/Apple? App developer? Public health authorities? Governments?

Through the les of Contextual Integrity

- Map flows: demand full transparency
- Assess against LEGITIMATE norms
- Reasonable expectations
- AND: how does the data flow promote health while minimizing harms to individuals
- Consent & anonymity approaches are neither necessary nor sufficient, but can be helpful mitigations as needed.