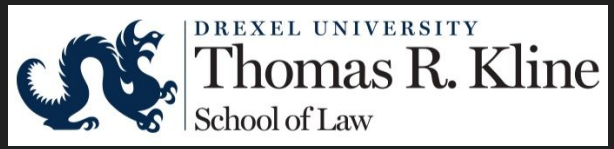
# Lessons in VCR Repair: Compliance of Android App Developers with the California Consumer Privacy Act (CCPA)

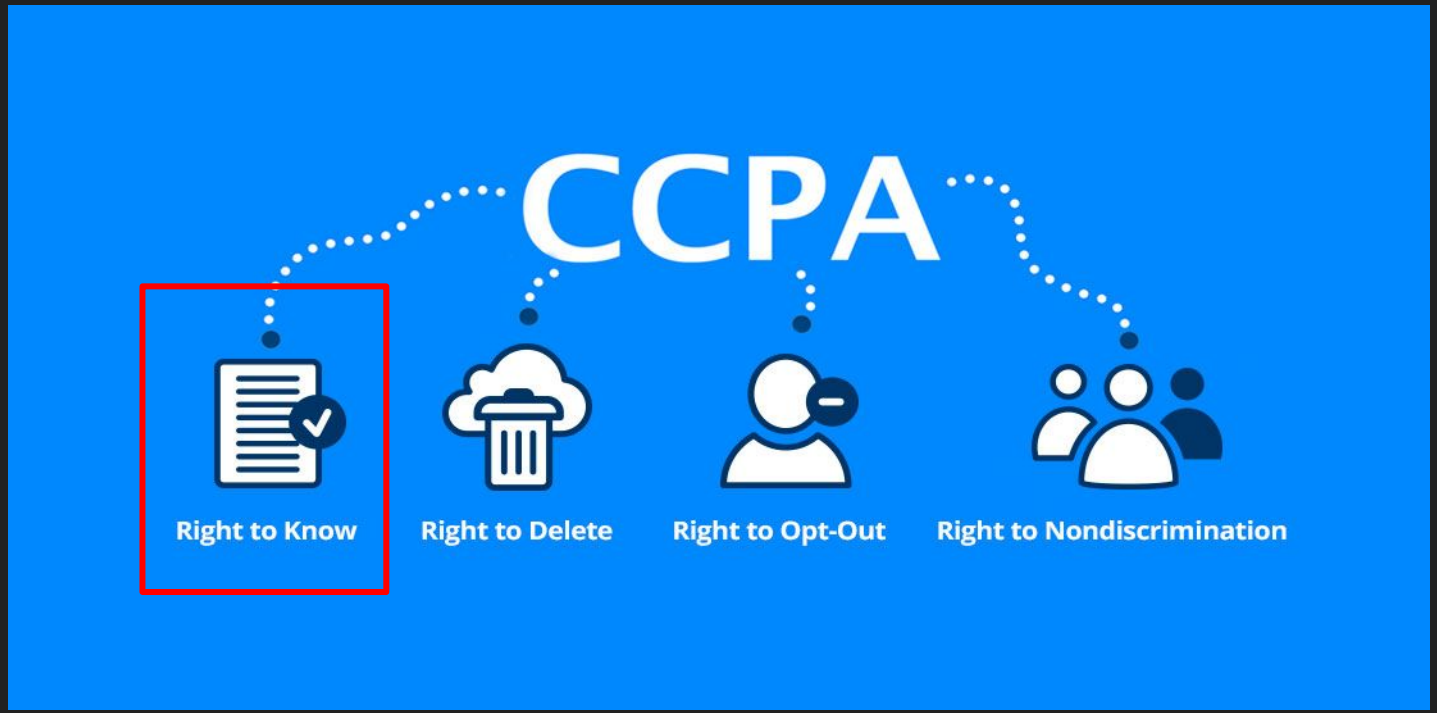
The 23rd Privacy Enhancing Technologies Symposium (PETS 23)

Nikita Samarin, Shayna Kothari, Zaina Siyed, Oscar Bjorkman, Reena Yuan, Primal Wijesekera, Noura Alomar, Jordan Fischer, Chris Hoofnagle, Serge Egelman



# California Consumer Privacy Act (CCPA)



# How does the CCPA compare to EU's GDPR?

## CCPA

- Applies only to for-profit businesses subject to additional criteria
- Right to know requires companies to provide data "in a portable [...] format"
- Consumers can request *specific* identifiable data collected about them
- Privacy policies only specify categories

## GDPR

- Applies broadly to entities that process Europeans' personal information
- Rights of access and portability are two distinct rights
- Consumers can request *specific* identifiable data collected about them
- Privacy policies only specify categories

# Why is the “right to know” so important to consumers?

- Enables other privacy rights
- May prompt consumers to change their privacy behavior
- Hold companies accountable to their stated information practices

# Research Questions

To what extent do Android app developers comply with the provisions of the California Consumer Privacy Act (CCPA) that require them to…

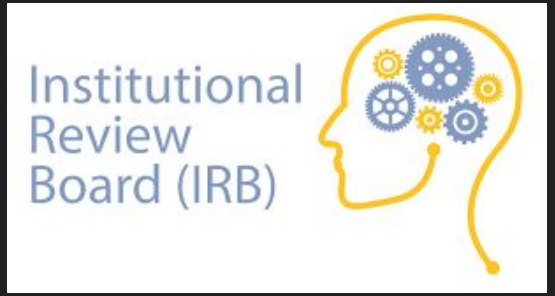
- respond to verifiable consumer requests (VCRs) by **accurately disclosing personal information** that they collected and shared about them?
- maintain **accurate privacy notices**?

# On ethical research conduct

We examined ethical issues surfaced by other work and shared our study methodology with the IRB* office at UC Berkeley

Our main objectives were:

- Determining which developers are subject to the CCPA
- Submitting requests to know that are legally valid




*This is not “human subjects research” and therefore beyond the purview of an IRB!

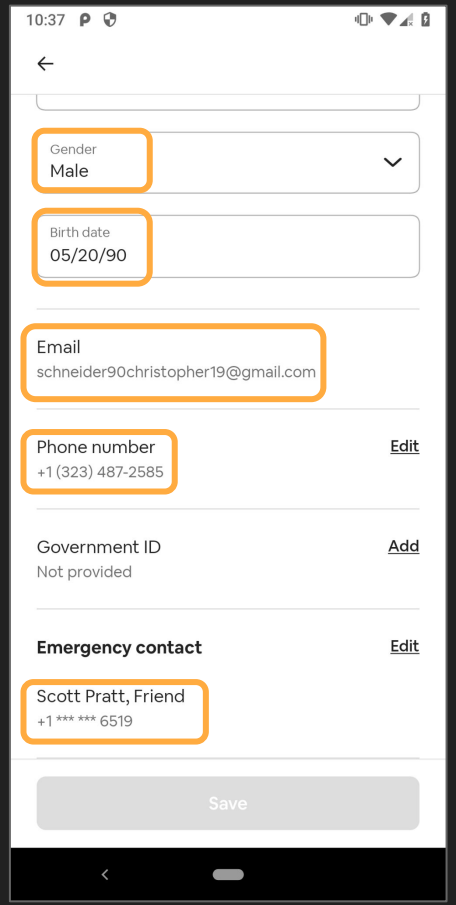
# CCPA has **threshold requirements** that are not easily publicly knowable

At the same time, **Sec. 5 of the FTC Act** prohibits "**deceptive acts or practices**," which include material representations that are likely to mislead consumers

We initially selected **160** top-ranked Android apps across 20 categories

We then narrowed down this dataset to **109** apps with **CCPA disclosures** in their privacy policies, which we also analyzed to determine each app's **information practices**

We then ran these apps and collected their **network traffic**



# We submitted verifiable consumer requests (VCR) using each app's prescribed procedures for submitting VCRs

**Initial Request**

[Subject] CCPA Request to Know Personal Information

Dear Privacy Compliance Officer,

My name is [*name*]. I live in California and I am exercising my data access rights under the California Consumer Privacy Act (CCPA) to obtain a copy of the categories and the specific pieces of personal information that [*company*] has collected about me.

# Pseudonyms

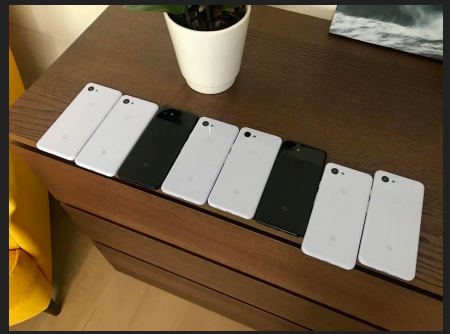
Mitigate two **confounding** variables

CCPA grants the right to know to California consumers, “a natural person who is a California resident [...], **however identified, including by any unique identifier**”

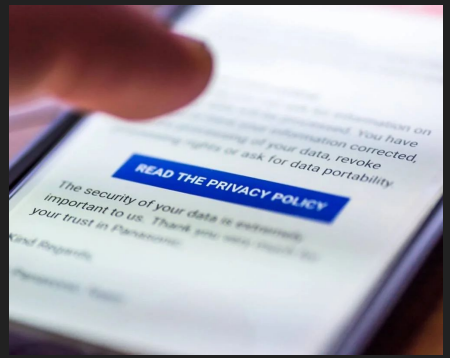
Our requests were **valid** because:

- They were only sent by researchers who are California residents
- Researchers testing the apps and submitting the requests were always identifiable by a unique identifier

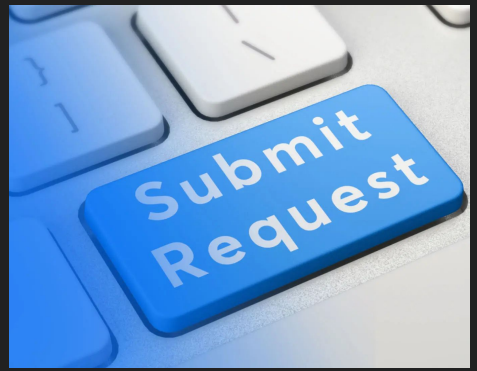
# Finally, we compared the **disclosed** and **actual** data practices



==




==




?

# What did we learn from submitting requests?

- **Two-thirds** of app developers provided **two or more** methods to submit requests (e.g., 65% = email; 39% = dedicated portal)
- In most cases, we were asked to provide **basic information** but some developers also requested **technical identifiers**
- Only **7** app vendors explicitly requested proof of California residency

# What did we learn from developer responses?

- Out of 109 requests, we received a material response from **80 developers** (21 = no reply, 5 = refused to verify, 3 = could not verify)
- Out of these 80 responses, we received our data in **69 cases** (8 = no data collected, 3 = check account profile)
- While **68** developers provided specific pieces of PI, only **25** named the categories of third parties to whom our information was sold or disclosed
- Only **6** companies presented the same data using two different formats for usability and portability purposes

# What did we learn from analyzing these responses?

- **8 developers** claimed not to collect any personal information, but **only one** appeared to not actually collect any data
- **68 developers** provided specific pieces of personal information, but **only 9** fully disclosed the extent of their data collection practices
- In their privacy policies, **25 (31%)** did not fully disclose the collection and **17 (21%)** did not fully disclose the sharing of information with third parties

# To summarize the compliance with the CCPA

Out of 109 companies:

- **34%** did not provide multiple means to submit requests
- **24%** did not respond to our request

Out of 69 companies responding with our data:

- **91%** did not provide data in a usable and a portable format
- **87%** did not fully disclose the personal information collected about us
- **64%** did not provide the categories of third parties

# Recommendations

## For developers:

- If possible, use existing authentication mechanisms to confirm the identity of the requester
- Secure access to and transmission of consumers' personal information
- Provide information in several formats (i.e., both human readable and portable)

## For regulators:

- Educate developers on what constitutes personal information
- Provide more guidance on the contents and the format of VCR responses

Thank you! Please reach out: nsamarin@berkeley.edu | @nsamarin | linkedin.com/in/nikitasamarin/

# Our work holds important implications:

For consumers:

- Determining the applicability of the CCPA is not trivial
- VCR responses lack uniformity across responses from different organizations

For developers:

- If possible, use existing authentication mechanisms to confirm the identity of the requester
- Secure access to and transmission of consumers' personal information (e.g., use 2FA, download links with time expiration, password-protected files)

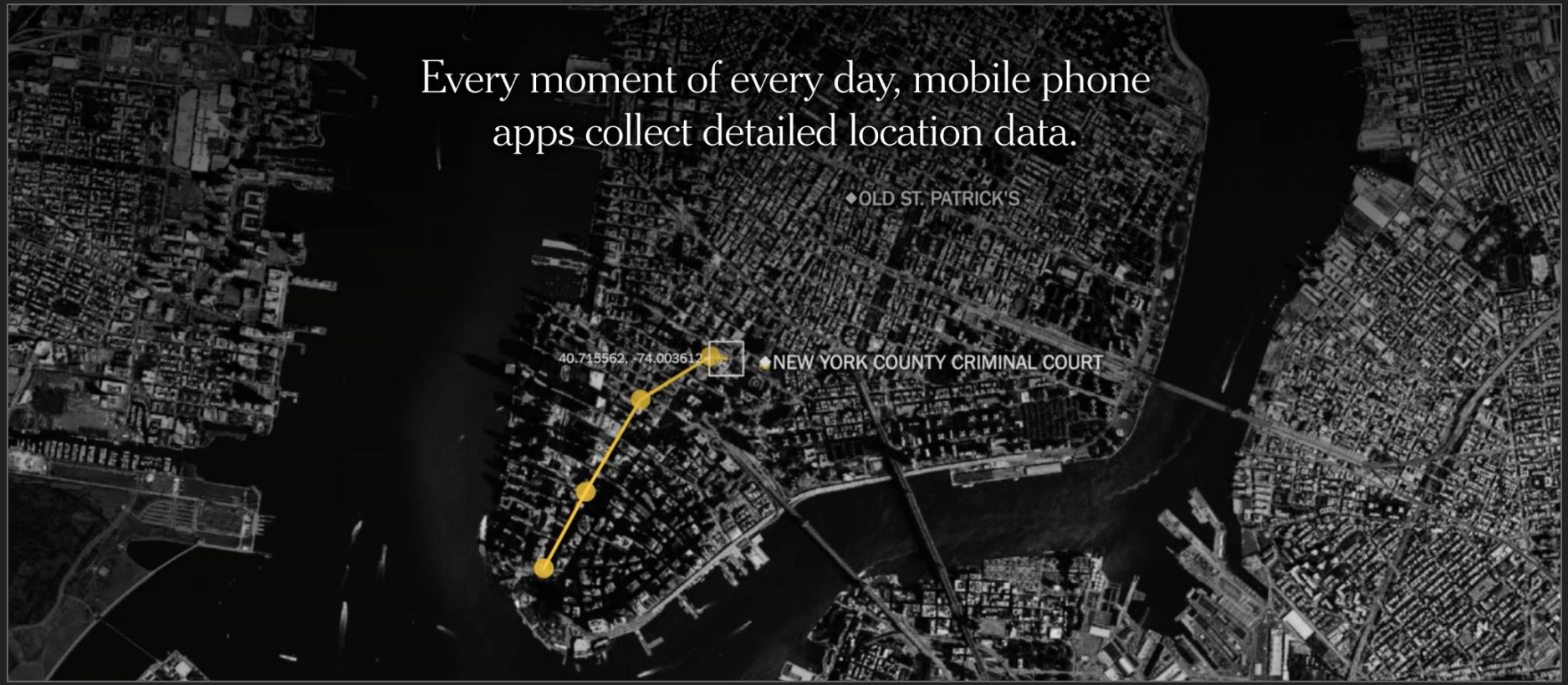
For regulators:

- Educate developers on what constitutes personal information
- Provide more guidance on the contents and the format of VCR responses

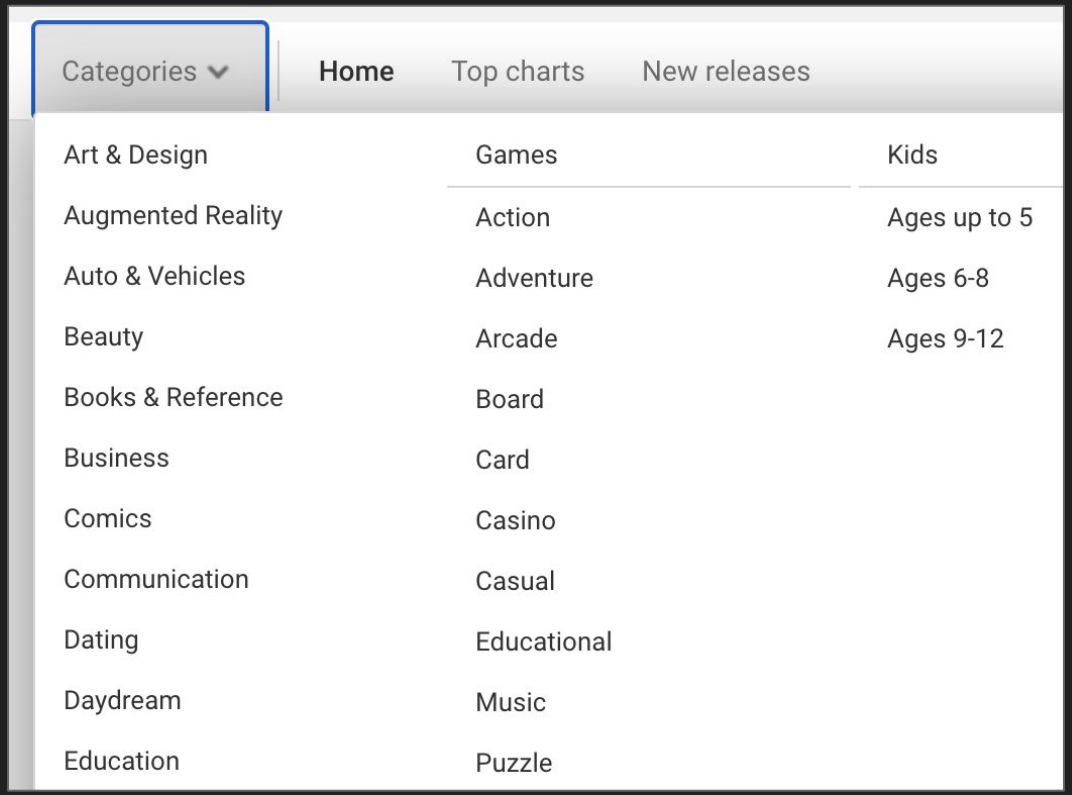
# Summary

- The “right to know” enables informed decision-making and exercising privacy rights
- We analyzed the network traffic, privacy policies, and responses to VCRs for 109 top-rated Android apps featuring CCPA-specific disclosures
- While developers provided specific pieces of personal information in VCR responses, many have omitted information associated with identifiers, geolocation, and sensory data
- Regulators should provide guidance to developers regarding the contents and format of VCR responses

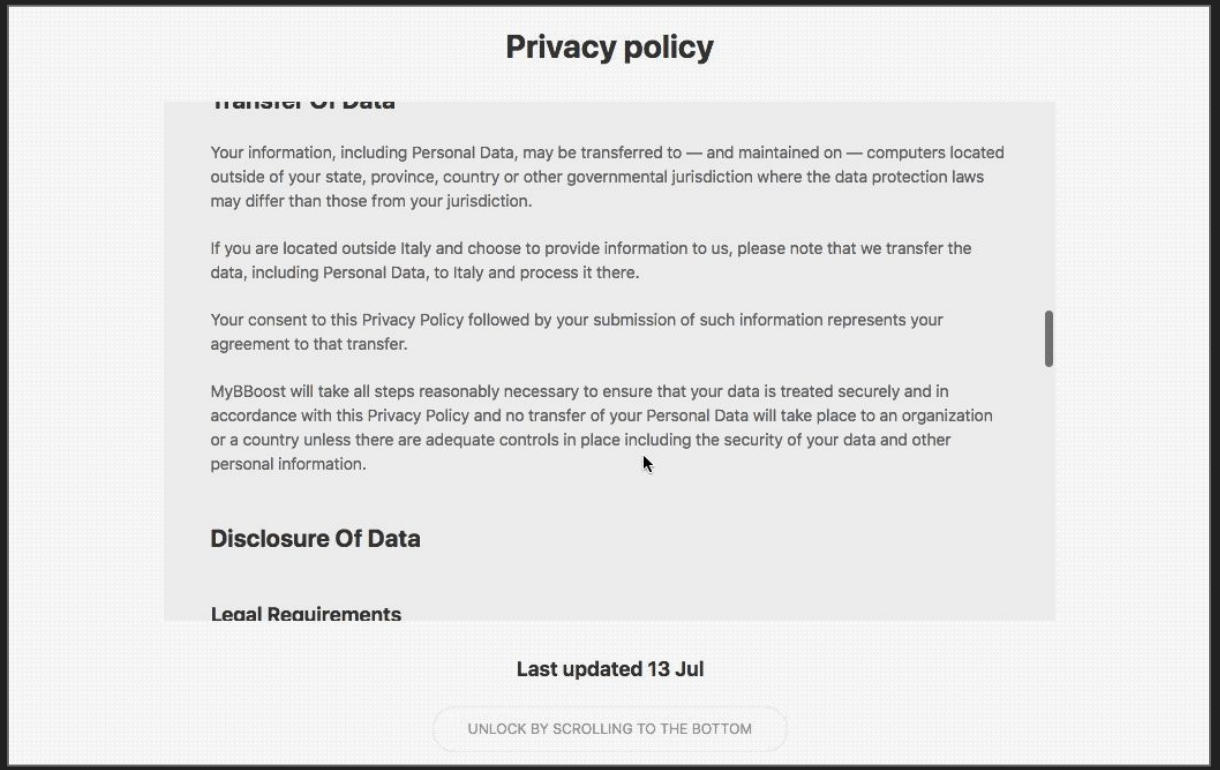
Thank you! Please reach out: nsamarin@berkeley.edu | @nsamarin | linkedin.com/in/nikitasamarin/


Every moment of every day, mobile phone apps collect detailed location data.
OLD ST. PATRICK'S
40.715562, -74.003612
NEW YORK COUNTY CRIMINAL COURT

# Initially, we selected **160 top-ranked** Android mobile apps



# And analyzed practices disclosed in privacy policies



Out of 80 (73%) companies that successfully responded to our VCRs:

- 69 (86%) provided data in response to our request, and only one of them did not provide specific pieces of personal information
  - However, compliance with other provisions of the “right to know” was less uniform
- Only 9 (11%) fully disclosed the extent of their data collection in reply to VCR
  - e.g., 21 apps did not disclose the collection of geolocation data
- In their privacy policies:
  - 25 (31%) did not fully disclose the collection of personal information
  - 17 (21%) did not fully disclose the sharing of information with third parties