Carnegie Mellon University

The Semantics of Privacy: From Privacy Policy Analysis to Code-Level Enforcement

Travis Breaux

in collaboration with Rocky Slavin, Mitra Bokaei Hosseini, Xue Qin, Jaspreet Bhatia, Xiaoyin Wang, Jianwei Niu

High Confidence Software and Systems
May 9, 2017
Annapolis, Maryland

institute for SOFTWARE RESEARCH

Problem and Motivation

- **Movement for increased accountability in privacy**: privacy by design, privacy engineering, responsible use
  - WH. Big Data Reports, NISTIR 8062, EU GDPR
- **Semantic gap between policy and code**: policy authors and auditors, and programmers who control code, use different semantics (Slavin et al., 2016)

R. Slavin, X. Wang, M.B. Hosseini, W. Hester, R. Krishnan, J. Bhatia, T.D. Breaux, J. Niu. "Toward a Framework for Detecting Privacy Policy Violation in Android Application Code," *38th ACM/IEEE International Software Engineering Conference (ICSE),* Austin, Texas, pp. 25-36, 2016.

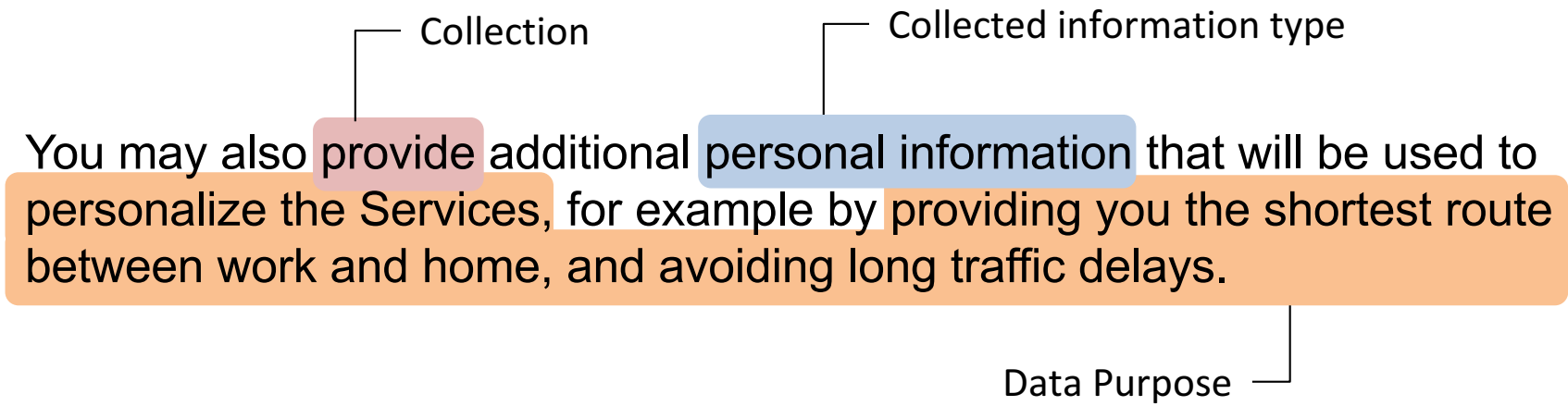
©2017 T.D. Breaux

Related Work

- **Android permission analysis**
  - PScout by Au et al., 2012 (80% of methods map to one permission)
  - Stowaway by Felt et al., 2011 (apps were 35% over-privileged)
  - Permission Check by Vidas et al., 2011
- **Android permissions and user expectations**
  - Lin et al., 2014 (flashlight app uses location)
- **Android policy generation and developer guidance**
  - PAGE by Rowen and Dehlinger, 2014
  - PermitMe by Bello-Oguna and Sheehab, 2014
- **Information flow analysis**
  - ScanDroid by Fuchs et al., 2009 (privacy leaks between apps)
  - TaintDroid by Enck et al., 2010 (runtime privacy leak detection)

©2017 T.D. Breaux

Assigning a formal semantics to policies



Specify:

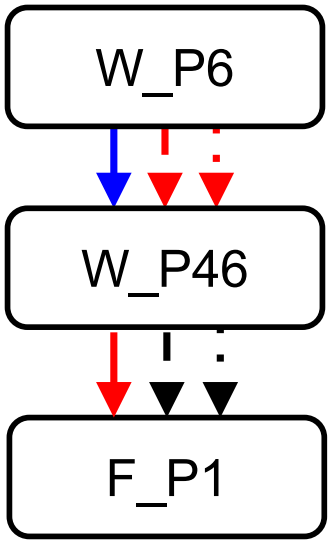
- COLLECT personal-information FROM waze-user FOR personalize-service
- personalize-service > providing-shortest-route
- personalize-service > avoiding-long-traffic-delays

Infer:

- Is a user's driving route a kind of personal information?
- For what purpose is driving route used?
- Is driving route shared with third party advertisers?

©2017 T.D. Breaux

Tracing multi-party data flows



COLLECT personal-information
FROM waze-user FOR enhancing-service-experience

TRANSFER unique-device-id
FROM anyone FOR anything TO ad-networks

COLLECT device-id, device-os, mac-address
FROM anyone FOR anything

Legend:

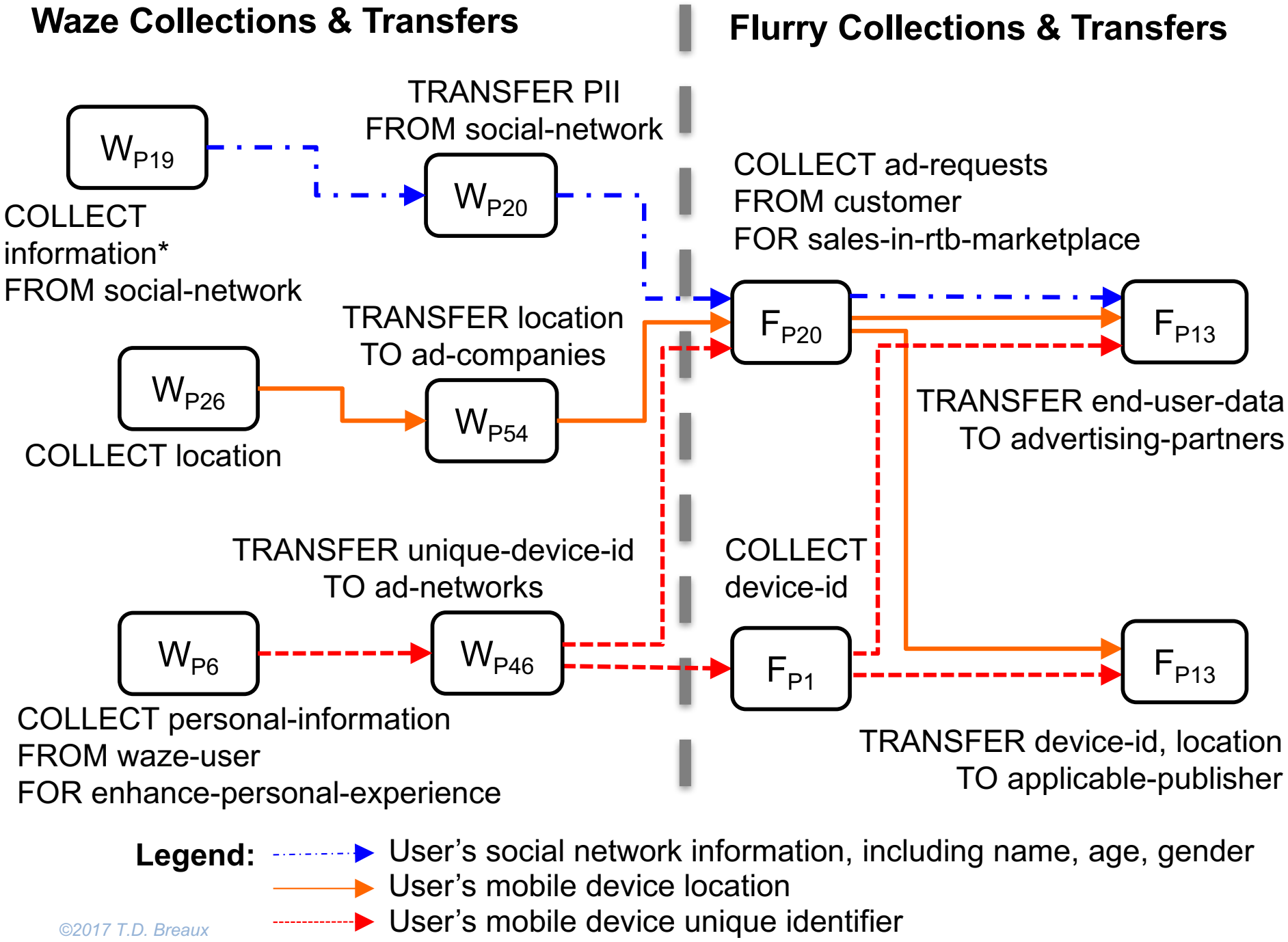
- ⟵ Data type
- ⟵ - - - - Data source
- ⟵ ..... Data Purpose

Blue: overflow
Red: underflow
Black: exact flow

Example from Waze and Flurry.com privacy policy

Travis D. Breaux, Daniel Smullen, Hanan Hibshi. "Detecting Repurposing and Over-collection in Multi-Party Privacy Requirements Specifications." *IEEE 23rd International Requirements Engineering Conference (RE'15)*, Ottawa, Canada, pp. 166-175, Sep. 2015.

©2017 T.D. Breaux



©2017 T.D. Breaux

Interlingua to align two policies

POLICY1 http://localhost/waze-pp.owl customer
POLICY2 http://localhost/flurry-pp.owl ad-networks

ads-clicked < aggregated-data
ads-clicked = clicks
ads-posted < aggregated-data
ads-viewed < aggregated-data
age = age
list-of-friends < end-user-data
location = location
personally-identifiable-information < end-user-data
profile-picture < end-user-data
unique-device-id = device-id

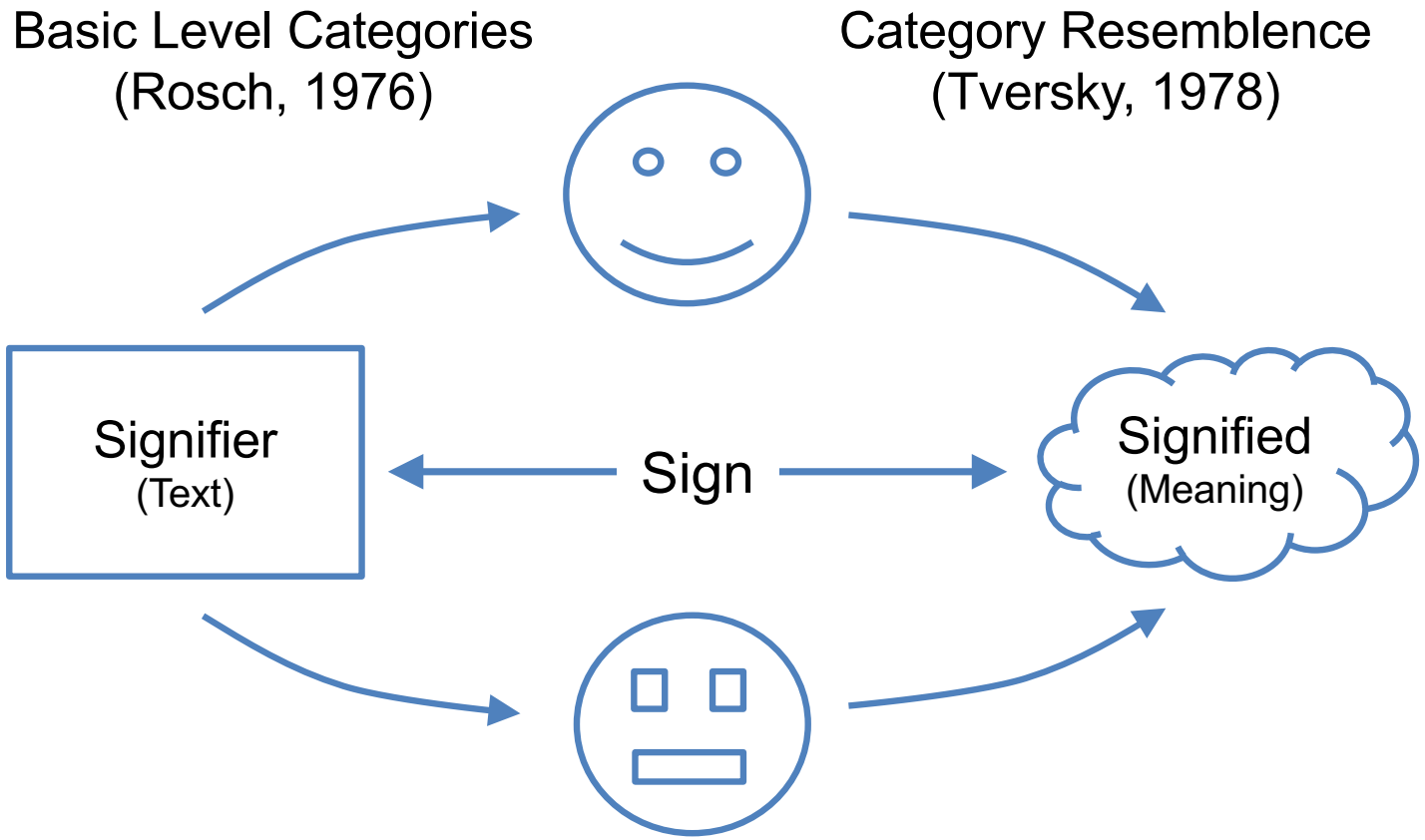
©2017 T.D. Breaux

Information Type Phrase	#
information	1867
personal information	1054
cookies	356
name	195
personally identifiable information	194
email address	148
data	121
contact information	77
protected health information	74
address	72
ip address	66
password	64
resume	63
non-personal information	58
location	52

Information Type Phrase	#
manufacturer	2
marketing effort responses	2
marketing information	2
marketing reports	2
marriott rewards information	2
marriott rewards number	2
media access control	2
member id-associated name	2
member information	2
message content	2
message data	2
message identifier information	2
message received	2
message sent	2
messages opened	2

©2017 T.D. Breaux

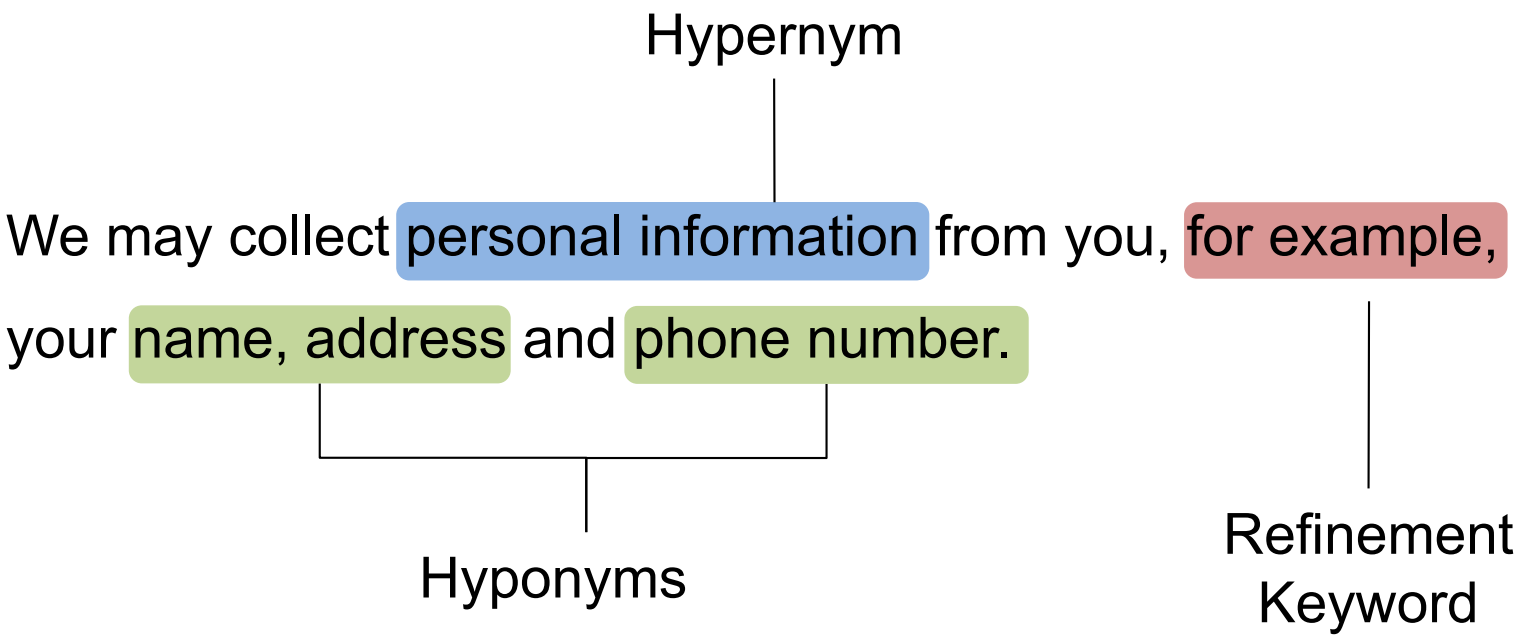
What do we mean by semantics?



Ferdinand de Saussure, *Course in General Linguistics*, 1916

©2017 T.D. Breaux

Hyponymy and Hearst Patterns



Excerpt from Barnes and Noble Policy, May 7, 2013.

M. A. Hearst, “Automatic acquisition of hyponyms from large text corpora,” *14th Conf. Computational Linguistics*, v. 2, 1992, pp. 539-545.

M. Evans, J. Bhatia, S. Wadkar, T.D. Breaux " An Evaluation of Constituency-based Hyponymy Extraction from Privacy Policies,” In Submission: *25th IEEE International Requirements Engineering Conference (RE'17),* Lisbon, Portugal, 2017

Example Tregex Pattern

(NP (PRP We))

(VP (MD may)

(VP (VB collect)

(NP (JJ personal) (NN information))

(PP (IN from)

(NP (PRP you)))

(, ,)

(PP (IN for)

(NP

(NP (NN example))

(, ,)

(NP (PRP$ your) (NN name) (, ,) (NN address)

(CC and)

(NN phone) (NN number))))))

This noun phrase (NP) is assigned to the variable "hypernym"

This prepositional phrase describes the keywords that indicate the hyponymy relation

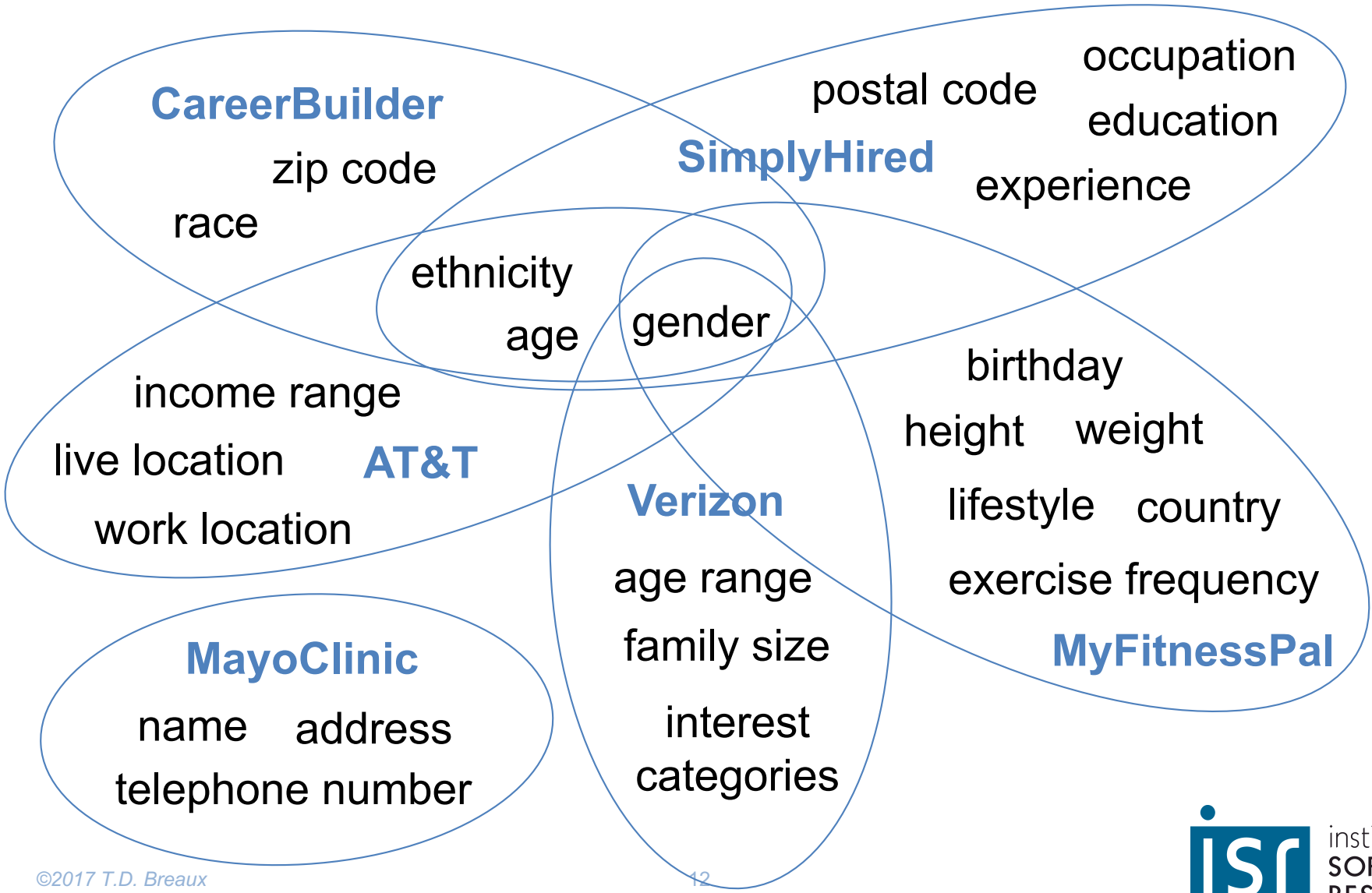
This noun phrase (NP) is assigned to the variable "hyponym"

* The A $ B means "A is a sibling of B" and the A < B means "A immediately dominates B"

Matching Tregex Pattern*

(NP=hypernym $ (IN < for) < (NP< (NN < example)) < NP=hyponym)

Demographic Information



©2017 T.D. Breaux

isr institute for SOFTWARE RESEARCH

Surveying ontology preferences

1. **browser** : **web browser type** ☐ click to swap word order
   - ○ is a part of
   - ○ is a kind of
   - ○ is equivalent to
   - ○ is unrelated to
   - ○ unsure or unclear

2. **contact** : **contact list** ☐ click to swap word order
   - ○ is a part of
   - ○ is a kind of
   - ○ is equivalent to
   - ○ is unrelated to
   - ○ unsure or unclear

3. **screen content** : **user content** ☐ click to swap word order
   - ○ is a part of
   - ○ is a kind of
   - ○ is equivalent to
   - ○ is unrelated to
   - ○ unsure or unclear

©2017 T.D. Breaux

Sample survey results

	P	W	H	O	E	U	X
browser : web browser type	3	11	3	3	9	0	1
contact : contact list	24	2	0	0	4	0	0
screen content : user content	6	2	4	6	4	6	2
mobile device: unique device id	3	19	1	2	2	2	1

P: Part-of
W: Whole-of
H: Hypernym-of (superclass)
O: Hyponym-of (subclass)

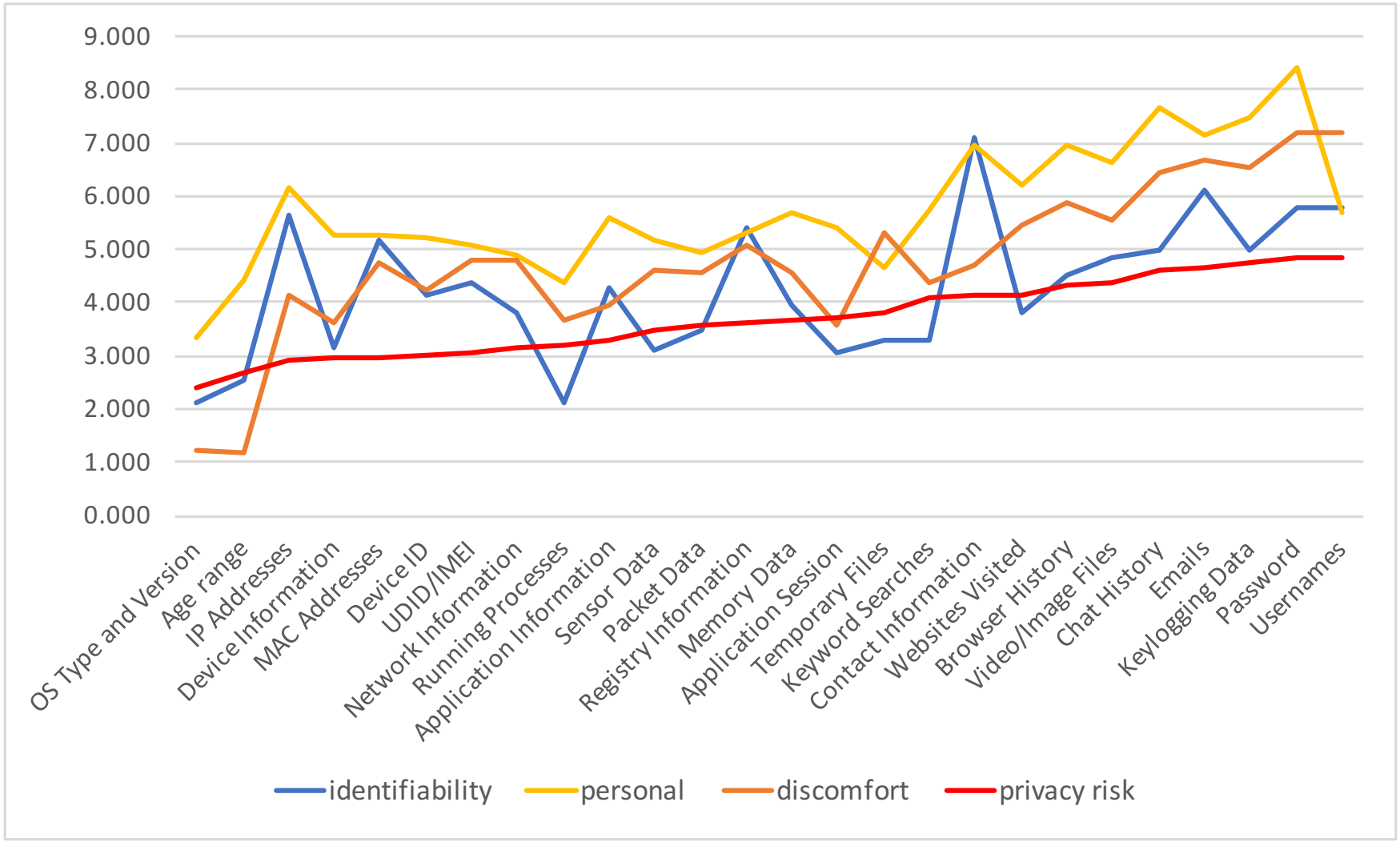
E: Equivalent-to
U: Unrelated
X: Unsure or unclear

Lexicon containing 351 unique information type phrases

Results: Precision=0.964, Recall=0.543
Among 639 false negatives, most require augmented semantics
Reduced paired comparisons by 7,719 or 12% of 62,853

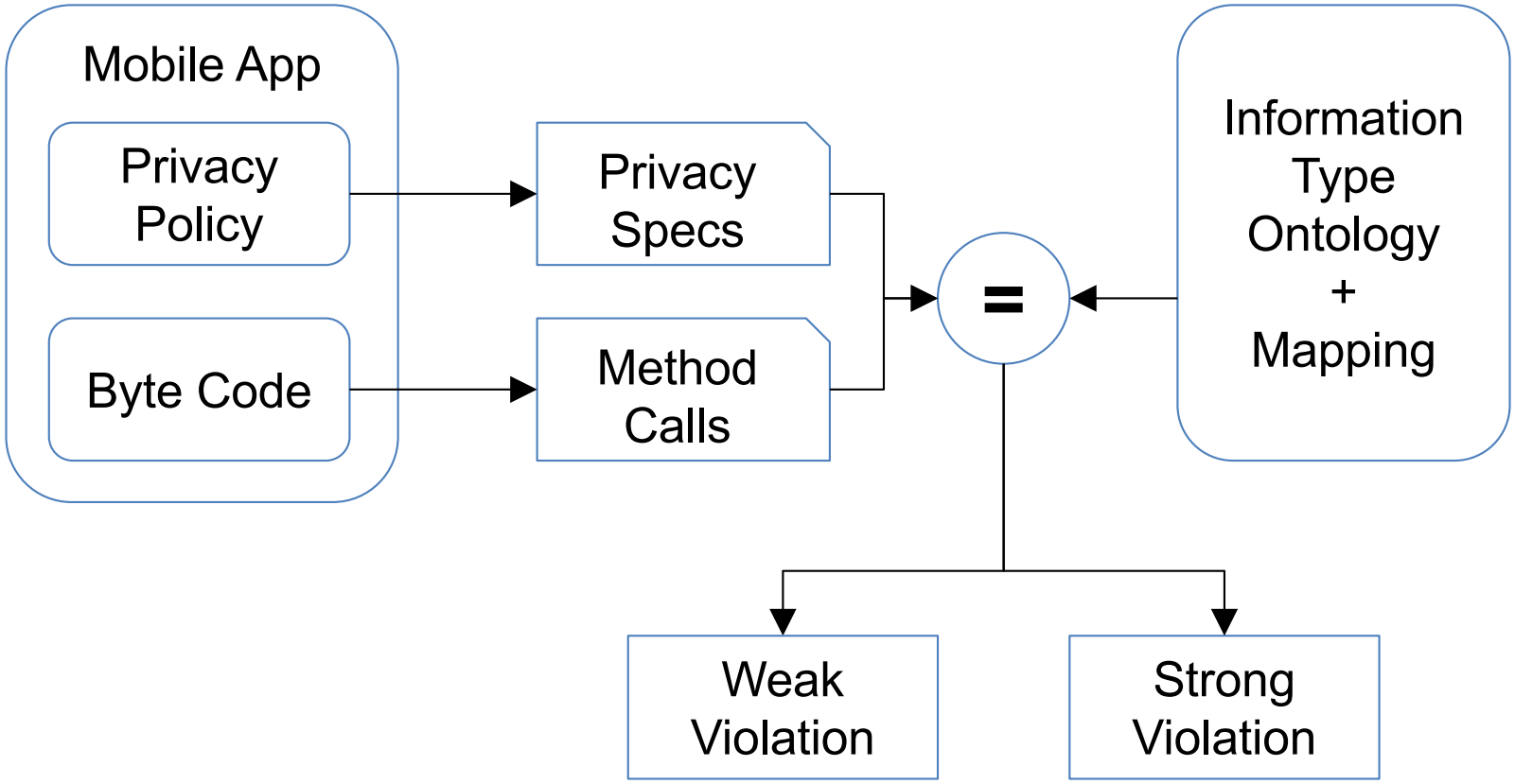
©2017 T.D. Breaux

Discomfort & Privacy Risk



©2017 T.D. Breaux

Aligning policy and code



R. Slavin, X. Wang, M.B. Hosseini, W. Hester, R. Krishnan, J. Bhatia, T.D. Breaux, J. Niu. "Toward a Framework for Detecting Privacy Policy Violation in Android Application Code," *38th ACM/IEEE International Software Engineering Conference (ICSE),* Austin, Texas, pp. 25-36, 2016.

©2017 T.D. Breaux

Example API docs annotation

Instructions: Select the noun phrases with your mouse cursor, if any, and then press one of the following keys when the phrase describes:

- Press ‘p’ for information related to personal privacy and accessed through the platform API

Method Descriptions:

android.location.Location.getAccuracy() – Get the estimated accuracy of this location, in meters.

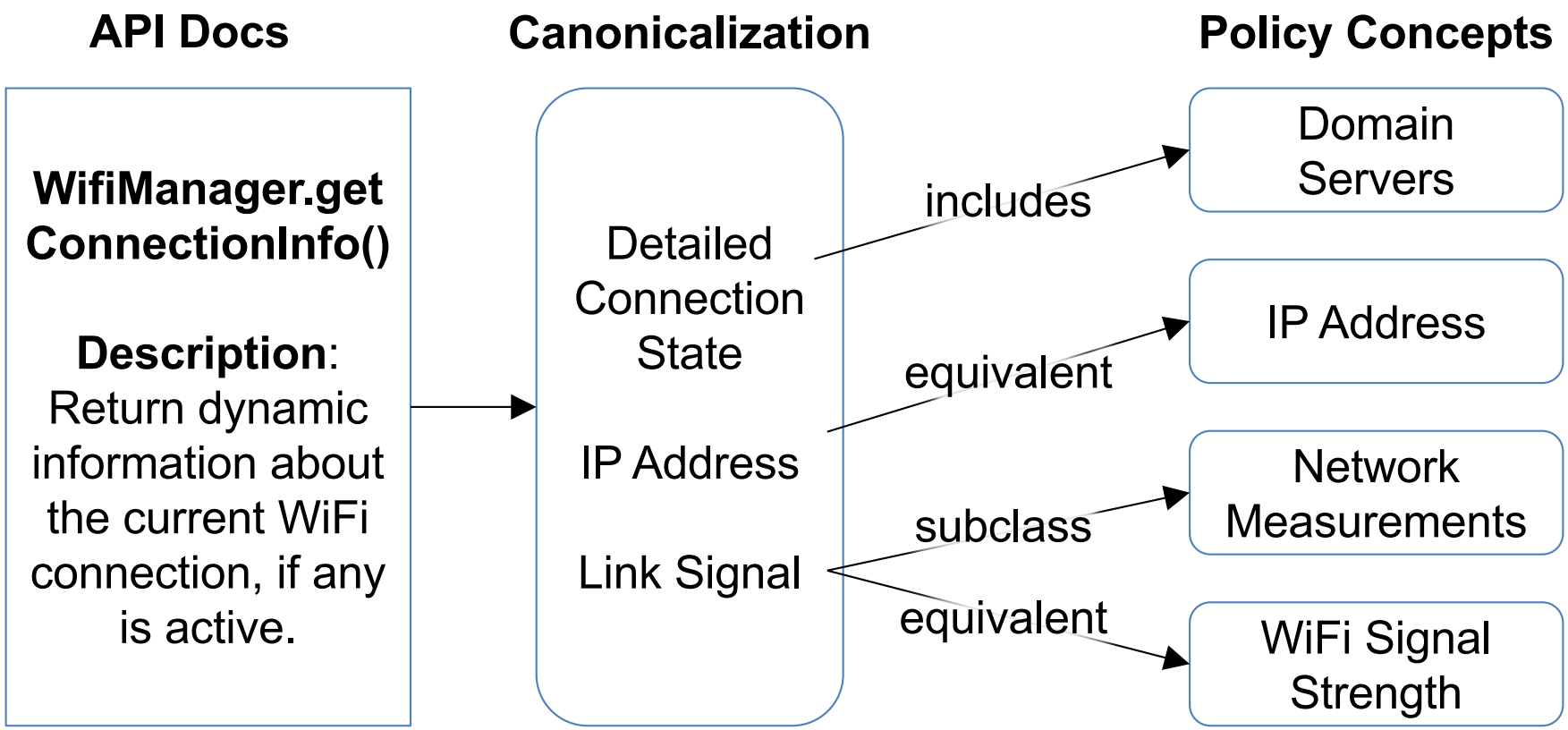
android.location.Location.setLongitude(double longitude) – Set the longitude in degrees.

android.location.Location.convert(double coordinate, int outputType) – Converts a coordinate to a String representation.

android.location.Location.getAltitude() – Get the altitude, if available, in meters above the WGS 84 reference ellipsoid.

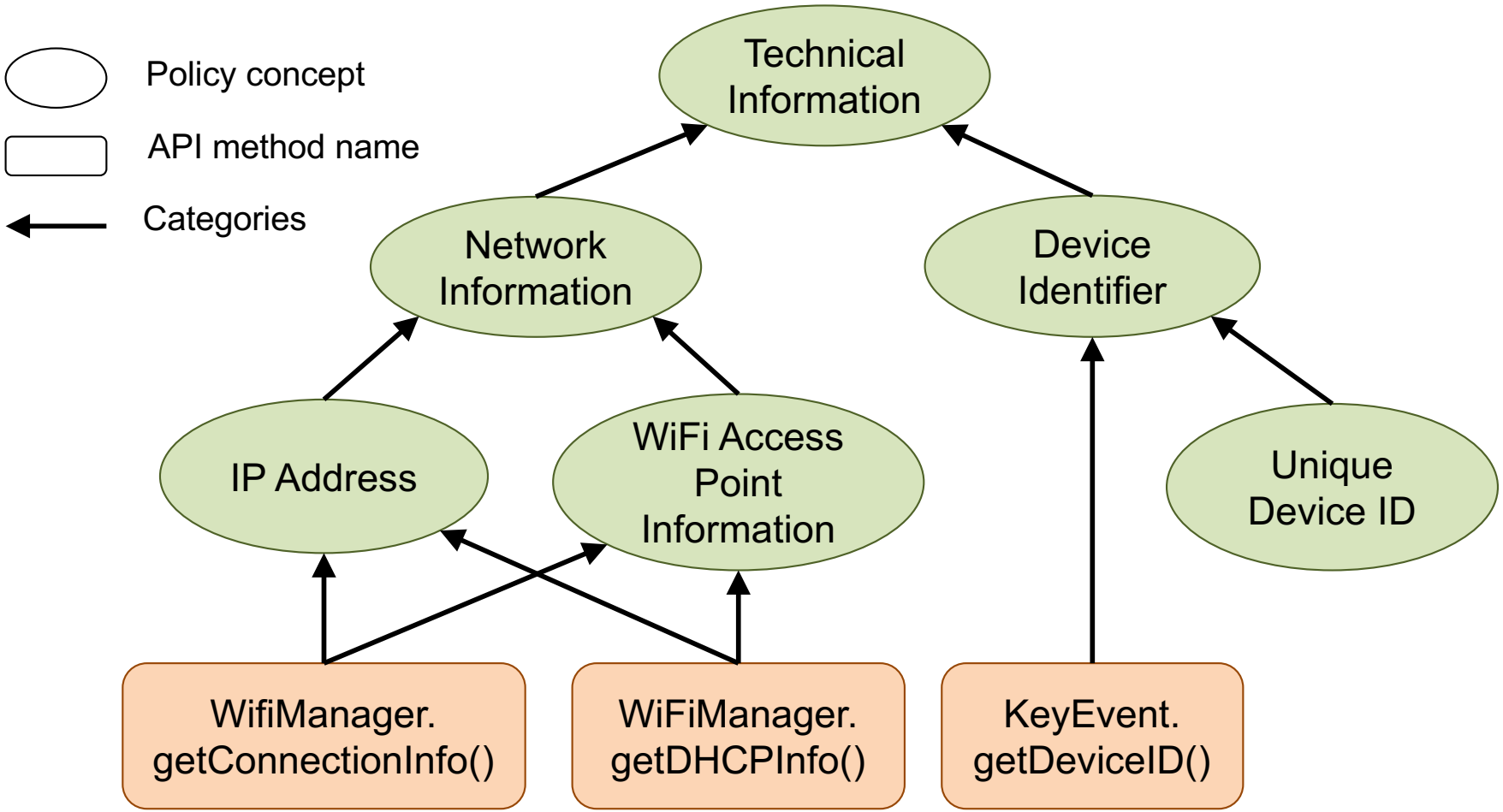
©2017 T.D. Breaux

Mapping API docs to policy terms



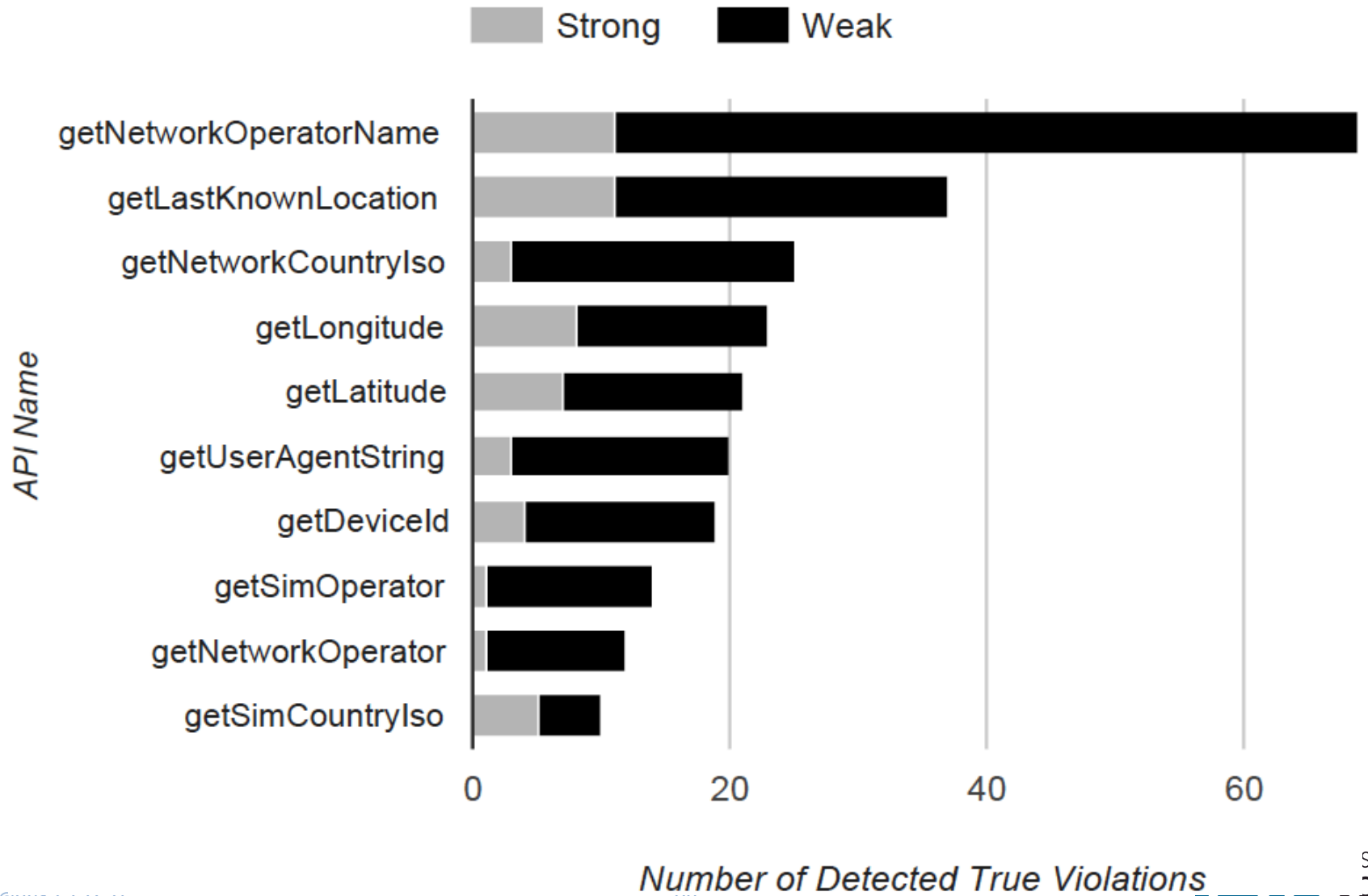
©2017 T.D. Breaux

Mapping APIs to policy terminology



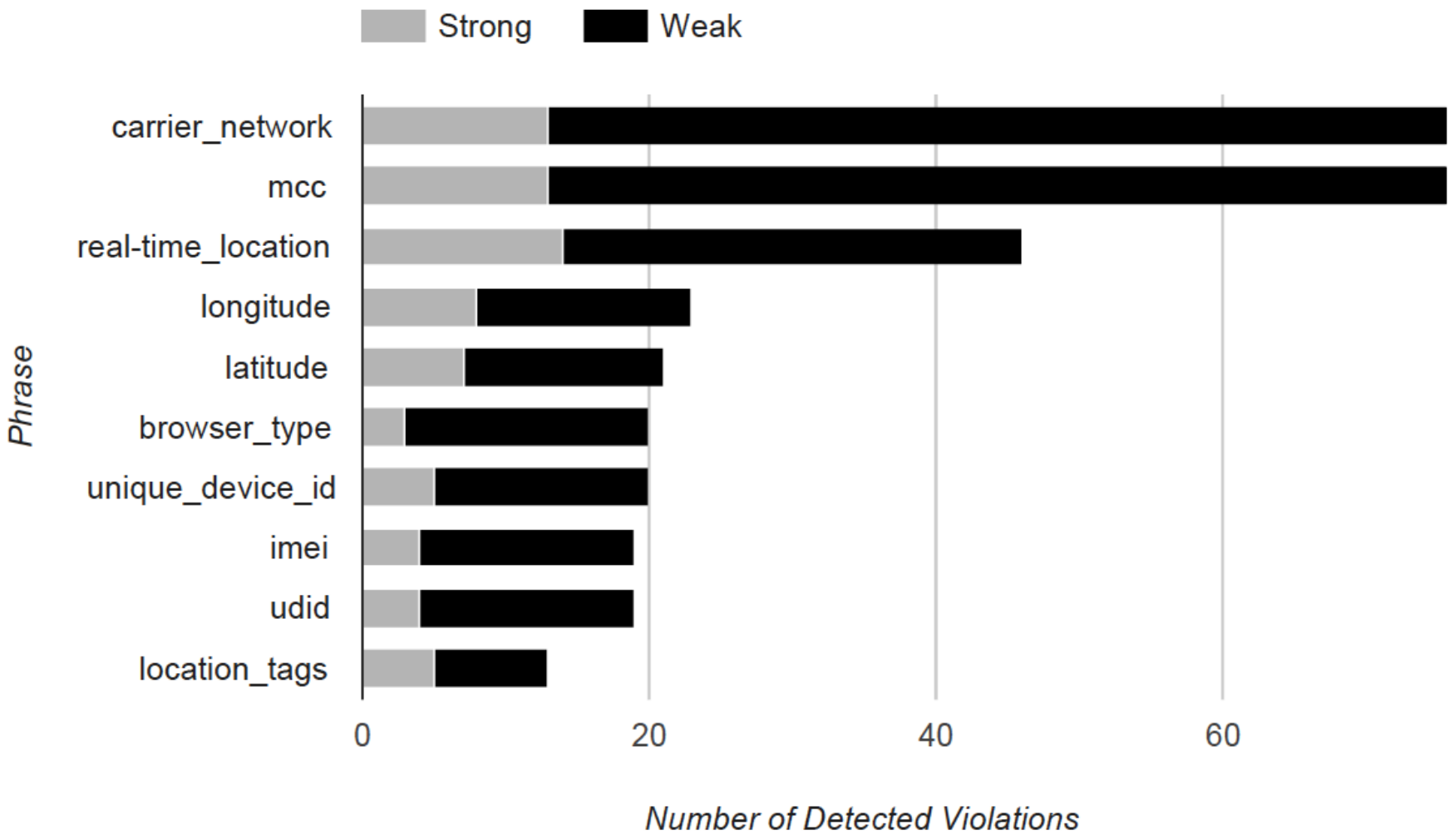
Slavin et al. “Toward a Framework for Detecting Privacy Policy Violations in Android Application Code,” ACM/IEEE International Conference on Software Engineering, pp. 25-36, 2016.

API methods with most violations



©2017 T.D. Breaux

Terminology with most violations



©2017 T.D. Breaux

Contributions and Future Work

- Overview of Results
  - For 477 Android apps, detected 55 strong and 267 weak policy violations, with accuracy 80%
- Information flow analysis
  - API method tracing for collection (relatively easy)
  - User-provided data tracing (harder)
  - Inferred, predicted or derived data (harder, still)
- Policy generation from code
  - Summarizing data practices – prioritizing disclosures by risk
  - Personalized policies and dialogue systems

©2017 T.D. Breaux

Questions

- This work was supported by NSA Award #141333, NSF Frontier Award #133059, ONR Award #N00244-16-1-0006

©2017 T.D. Breaux