



Australia's National Science Agency

{Privacy Policy} in Practice: Challenges, Implications, and Solutions

Shidong Pan

University of Edinburgh

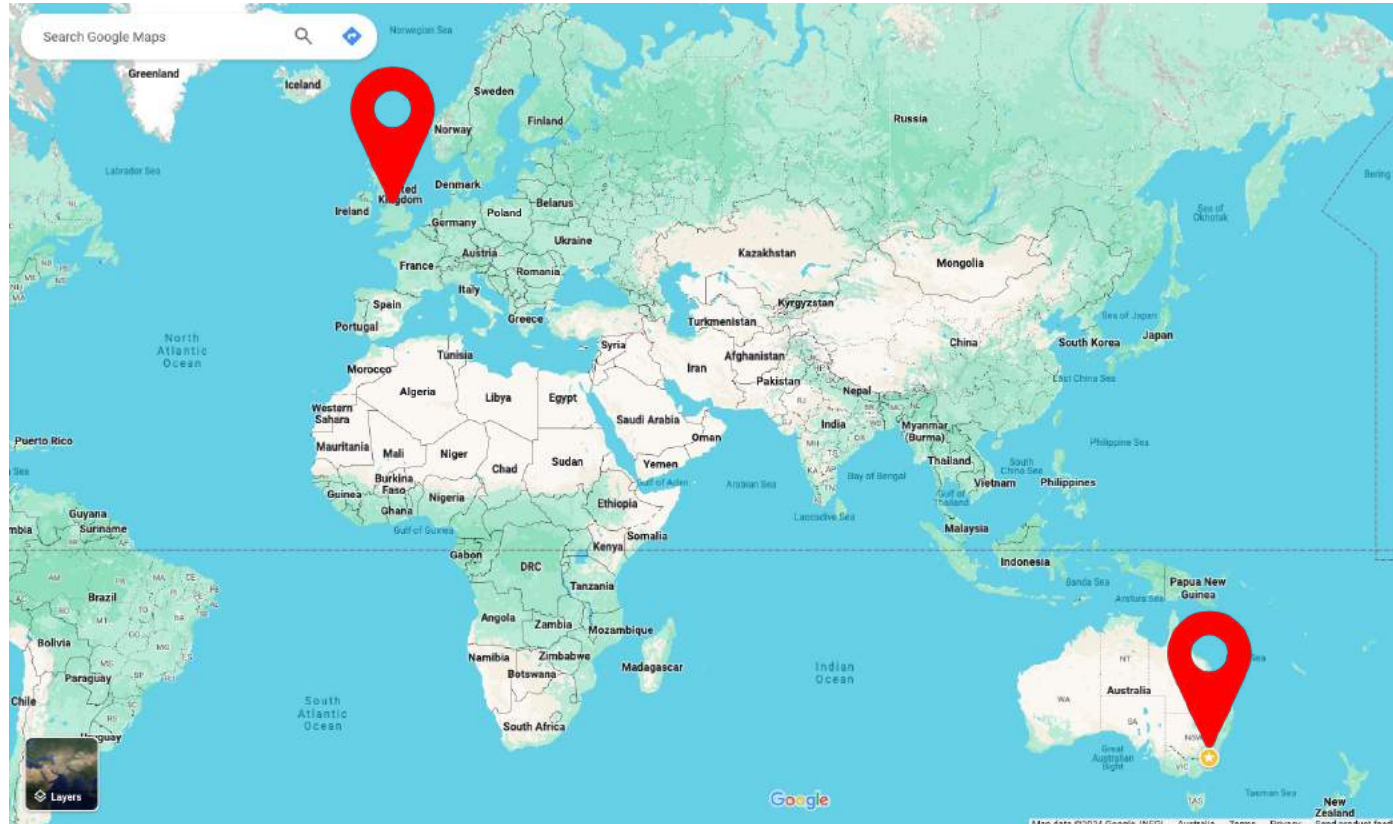
March 2024

Self-introduction



- Shidong Pan
- Bachelor of Advanced Computing @ ANU + Shandong University
- Master of Machine Learning & Computer Vision @ ANU
- Currently, I'm an about-to-finish PhD affiliated to:
 - School of Computing, ANU
 - Responsible AI Group, CSIRO's Data61
- Was a visiting PhD student at Singapore Management University (SMU).

Greetings from “downstairs” :)



Outline

1. Background and Motivation

2. Current Privacy Policy Research Landscape

- Content Analysis (PP Descriptions - Software Behaviours)
- Compliance Checking (PP Descriptions - Law/Reg Requirements)
- Transparency and Readability of PP and Privacy Notices

3. My Research Projects

- An empirical study of Online Automated Privacy Policy Generators
- Contextual Privacy Policy for Mobile applications

Privacy issues are making headlines everyday!

If You've Got a New Car, It's a Data Privacy Nightmare

Bad news: your car is a spy. It's

By **Thomas Germain** Published Yesterday



Norway court rules against Facebook owner Meta in privacy case

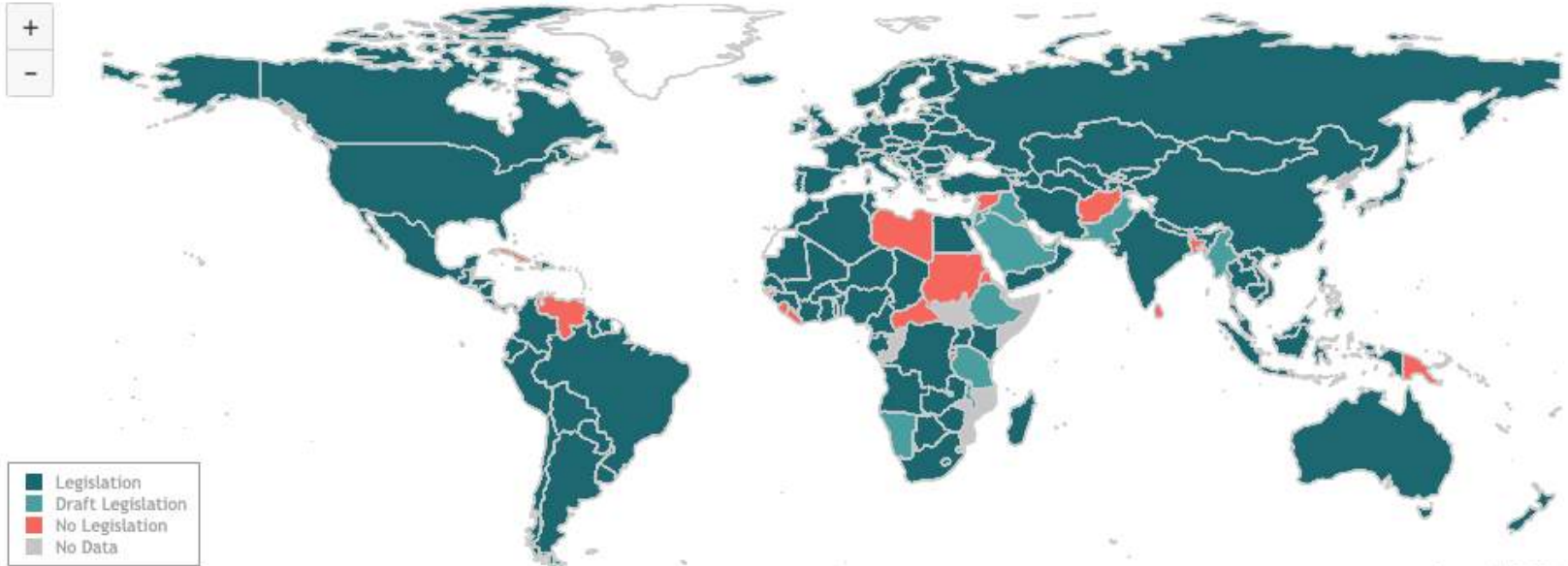


A screenshot of a news article. The top navigation bar includes 'Sport', 'Culture', 'Lifestyle', and 'More'. Below the navigation, there are sub-sections for 'Asia', 'Australia', 'Middle East', 'Africa', 'Inequality', and 'Global development'. The main headline reads: 'TikTok opens datacentre in Dublin in bid to combat European privacy concerns'. A sub-headline below it says: 'The Chinese-owned app also announced a UK-based cybersecurity company will independently audit data controls and protections'.



Privacy Laws and Regulations

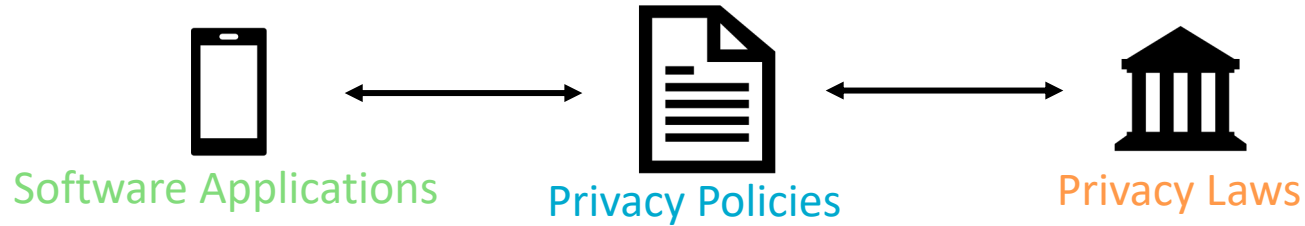
Data Protection and Privacy Legislation Worldwide



Source: UNCTAD, 14/12/2021

According UNCTD, 137 out of 194 countries had put in place legislation to secure the protection of data and privacy.

The Privacy Policy is essential and critical!



An APP entity must have a clearly expressed and up to date policy (the APP **privacy policy**) about the management of personal information by the entity [APP 1.3]

In re Google Assistant Privacy Litigation

457 F. Supp. 3d 797 - Dist. Court, ND California, 2020 - Google Scholar

... with our **Privacy Policy** and other appropriate **confidentiality** and security ... **Privacy Policy** Litig., 58 F. Supp. ... 2012) (finding no invasion of **privacy** based on Defendants' disclosure of each ...

☆ Save 📄 Cite Cited by 64 How cited All 2 versions

In re Facebook, Inc. Internet Tracking Litigation

956 F.3d 589 - Court of Appeals, 9th Circuit, 2020 - Google Scholar

... First, the December 2010 **Privacy Policy** does not contain any agreement that Facebook would not track ... [11] Second, and more generally, the **Privacy** and Data Use **Policies** do not ...

☆ Save 📄 Cite Cited by 267 How cited All 2 versions

Kauders v. Uber Technologies, Inc.

486 Mass. 557, 159 NE 3d 1033 - Mass: Supreme Judicial Court, 2021 - Google Scholar

... general principles of state contract law as **rules** of decision ... the link to the terms and conditions and the **privacy policy** ... question then becomes whether this type of **notice** was reasonable ...

☆ Save 📄 Cite Cited by 54 How cited All 2 versions

Examples of privacy policies

The screenshot shows the Meta Privacy Center interface. On the left is a navigation sidebar with the following items: 'Manage your accounts Accounts Center', 'Privacy Center home', 'Search', and 'Privacy Policy'. The main content area is titled 'Privacy Policy' and includes a sub-header 'What is the Privacy Policy and what does it cover?'. Below this, there is a 'Highlights' section with a star icon. The main text explains that Meta wants users to understand information collection and usage, and provides links to a printable version and previous versions. It also includes sections for 'What Products does this policy cover?', 'Learn more in Privacy Center about managing your privacy', and 'What information do we collect?'. A second 'Highlights' section is visible at the bottom of the main content area.

Facebook/Meta
> 20,000 words

The screenshot shows a simple, clean privacy policy document. The title 'Privacy Policy' is centered at the top in a large blue font. Below the title, there is a short introductory paragraph: 'This is the general privacy policy of my applications which is applicable to all the apps that I have on Google Play Store.' This is followed by a section titled 'Privacy Policy explains:' with three bullet points: 'What information we collect and why we collect it.', 'How we use that information.', and 'The choice we offer, including how to access and update information.' Below this is an 'Important:' section with a paragraph explaining that permissions are optional and not mandatory for app functionality. This is followed by a 'Permissions:' section with a paragraph stating that permissions are explained in each application and that none are mandatory. The document concludes with a sentence: 'For any further queries, please do email me at developer contact email address.'

Easy Communication
1k installs, 156 words

People do not read privacy policies!

- Privacy policies are very lengthy and detailed. The average length for popular app is about **4,000 words**.
- About **74% users don't read** privacy policy. For those who read it, the average reading time is 73 seconds [1].



The Hobbit: An Unexpected Journey (2012)

Thus, **user-centric** privacy notice and the **usable privacy** technology are pressingly needed.



[1] Jonathan A. Obar. 2016. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. SSRN Electronic Journal (2016). <https://doi.org/10.2139/ssrn.2757465>

Privacy Policies are commonly problematic!

POLIGRAPH: Automated Privacy Policy Analysis

Hao (ar
Detection of Inconsistencies in Privacy Practices of
Browser Extensions

<https://w>

Scrutinizing Privacy Policy Compliance of Virtual Personal Assistant Apps



Abstract—All major
provide additional func
experience while the ext
during their web browsi

Fuman Xie
University of Queensland
Australia

Suwan Li
Nanjing University
China

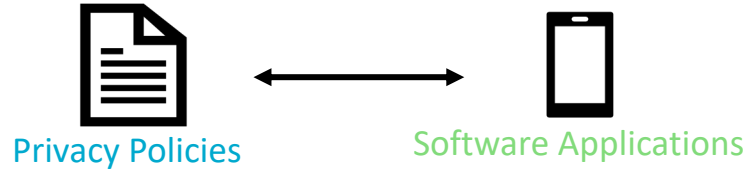
Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning

Hamza Harkous, *École Polytechnique Fédérale de Lausanne (EPFL)*;
Kassem Fawaz, *University of Wisconsin-Madison*; Rémi Leuret, *École Polytechnique Fédérale
de Lausanne (EPFL)*; Florian Schaub and Kang G. Shin, *University of Michigan*;
Karl Aberer, *École Polytechnique Fédérale de Lausanne (EPFL)*

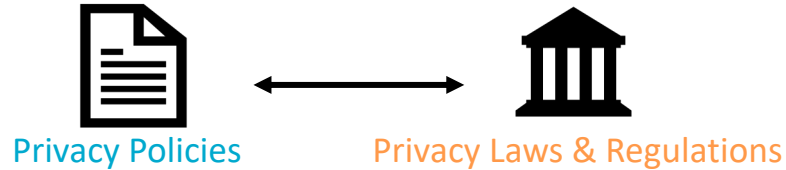
<https://www.usenix.org/conference/usenixsecurity18/presentation/harkous>

Privacy Policy Research Landscape

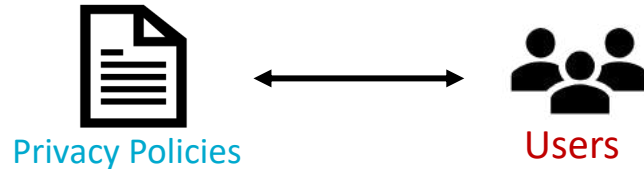
1. Content Analysis (PP Descriptions - Software Behaviours):



2. Compliance Checking (PP Descriptions - Law/Reg Requirements)

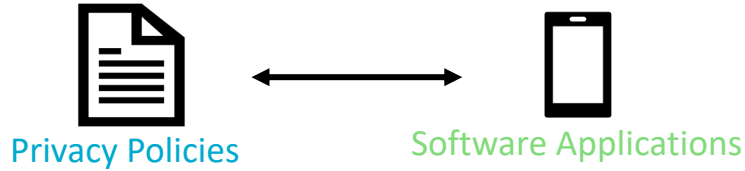


3. Transparency and Readability of PP and Privacy Notices:



Privacy Policy Research Landscape

1. Content Analysis (PP Descriptions - Software Behaviours):



2. Compliance Checking (PP Descriptions - Law/Reg Requirements)

3. Transparency and Readability of PP and Privacy Notices:

A Typical Framework of PP Content Analysis

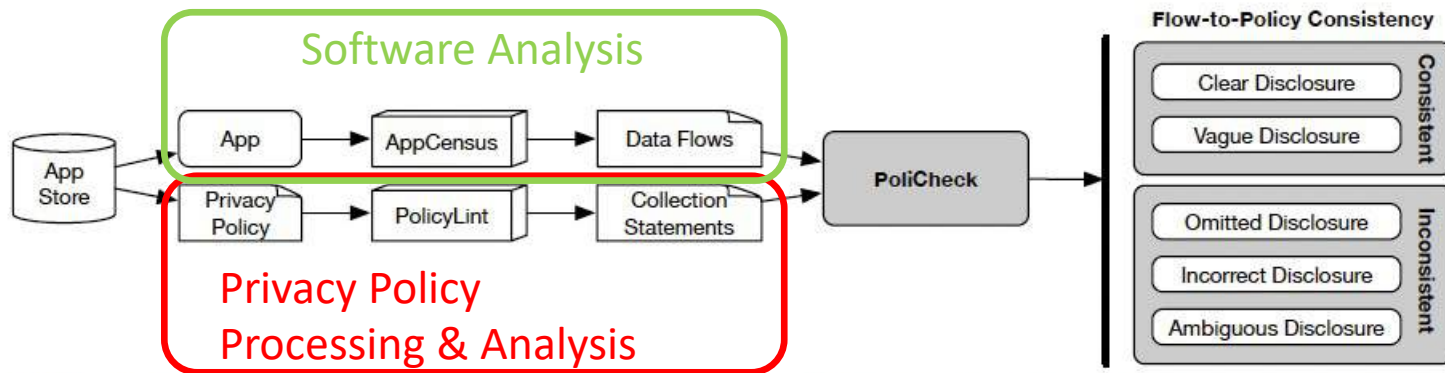


Figure 1: POLICHECK determines the consistency of a mobile application's data flows to its privacy policy.

Privacy Policy Content Analysis

Year	Name	Method	Authors	Venue
2016	OPP-115	Machine Learning (LR, SVM, HMM)	Wilson et al.	ACL
2018	Polisis	Deep Learning (CNN + DenseNet)	Harkous et al.	Security
2019	PolicyLint	Sentence-level NLP (NER, DND, etc.)	Andow et al.	Security
2021	PurPliance	Rule-based matching (NER, Pattern Detect)	Bui et al.	CCS
2023	PoliGraph	Rule-based matching (KG)	Cui et al.	Security

A Taxonomy of Privacy Policy Content

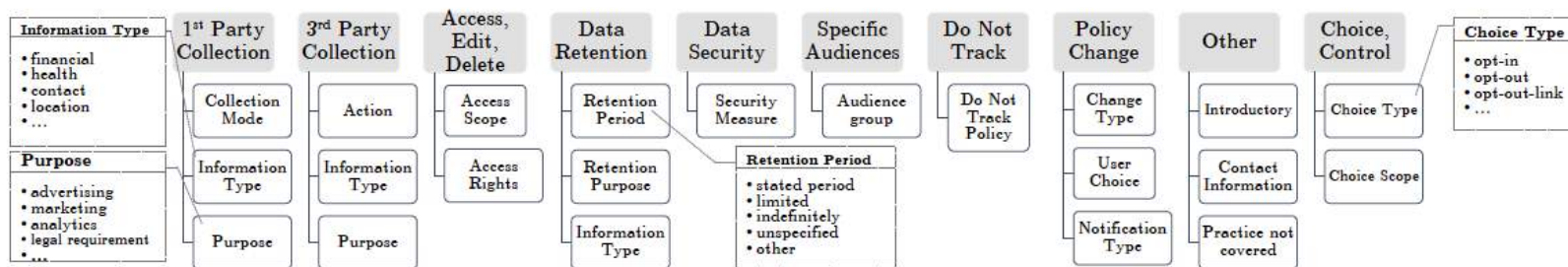


Fig. 3: The privacy taxonomy of Wilson *et al.* [11]. The top level of the hierarchy (shaded blocks) defines high-level privacy categories. The lower level defines a set of privacy attributes, each assuming a set of values. We show examples of values for some of the attributes.

Table 3: Classification *Precision/Recall/F1* (respectively abbreviated as P/R/F) for every single category, and their *Macro Average* of OPP-115 by Polisis [13], LR, SVM and HMM [6].

Label	Polisis			LR			SVM			HMM		
	P	R	F	P	R	F	P	R	F	P	R	F
1st Party Collection	0.79	0.79	0.79	0.73	0.67	0.70	0.76	0.73	0.75	0.69	0.76	0.72
3rd Party Sharing	0.79	0.80	0.79	0.64	0.63	0.63	0.67	0.73	0.70	0.63	0.61	0.62
User Choice/Control	0.74	0.74	0.74	0.45	0.62	0.52	0.65	0.58	0.61	0.47	0.33	0.39
Access, Edit, Deletion	0.89	0.75	0.80	0.47	0.71	0.57	0.67	0.56	0.61	0.48	0.42	0.45
Data Retention	0.83	0.66	0.71	0.10	0.35	0.16	0.12	0.12	0.12	0.08	0.12	0.09
Data Security	0.88	0.83	0.85	0.48	0.75	0.59	0.66	0.67	0.67	0.67	0.53	0.59
Policy Change	0.95	0.84	0.88	0.59	0.83	0.69	0.66	0.88	0.75	0.52	0.68	0.59
Do Not Track	0.94	0.97	0.95	0.45	1.0	0.62	1.0	1.0	1.0	0.45	0.40	0.41
Specific Audiences	0.96	0.94	0.95	0.49	0.69	0.57	0.70	0.70	0.70	0.67	0.66	0.66
<i>Macro Average</i>	0.85	0.79	0.81	0.49	0.69	0.56	0.65	0.66	0.66	0.52	0.50	0.50

Non-LLM Models

Table 1: Classification *Precision/Recall/F1* (respectively abbreviated as P/R/F) for every single category, their *Macro Average*, and the total *Accuracy* of OPP-115 by ChatGPT, GPT4 and Claude2.

Label	ChatGPT			GPT4			Claude2		
	P	R	F	P	R	F	P	R	F
1st Party Collection	0.94	0.90	0.92	0.98	0.97	0.97	0.99	0.65	0.78
3rd Party Sharing	0.92	0.90	0.91	0.97	0.95	0.96	0.69	0.98	0.81
User Choice/Control	0.92	0.90	0.91	0.92	0.98	0.95	0.77	0.63	0.69
Access, Edit, Deletion	0.89	0.99	0.94	0.92	0.99	0.96	0.87	0.84	0.85
Data Retention	0.93	0.96	0.95	1.00	0.81	0.89	1.00	0.96	0.98
Data Security	0.79	0.96	0.86	0.98	0.97	0.97	0.84	0.85	0.85
Policy Change	0.96	0.99	0.98	1.00	0.99	1.00	0.94	0.68	0.79
Do Not Track	0.91	1.00	0.95	1.00	1.00	1.00	1.00	0.35	0.52
Specific Audiences	1.00	0.92	0.96	1.00	0.95	0.97	0.93	0.79	0.86
Other	0.92	1.00	0.96	0.99	1.00	0.99	0.96	1.00	0.98
<i>Accuracy</i>	0.92						0.97		
<i>Macro Average</i>	0.92	0.95	0.93	0.98	0.96	0.97	0.90	0.77	0.81

LLMs



Software (mobile apps) Privacy Behaviour Analysis

Year	Name	Method/Intro	Authors	Venue
2020	PoliCheck	Android apps entity-sensitive policy and data-flow Analysis	Andow et al.	Security
2021	PrivacyFlash Pro	iOS apps data-flow to disclosure	Zimmeck et al	NDSS
2023	Lalaine	iOS apps data-flow to privacy-label	Xiao et al.	Security
2024	Matcha	Android app IDE In-IDE data/permission usage to privacy-label	Li et al. 2024	IMWUT

Content Analysis tools

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple/DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 <plist version="1.0">
4 <dict>
5   <key>NSLocationWhenInUseUsageDescriptions</key>
6   <string>We are using your location to recommend a gym nearby.</string>
```

A. iOS API Evidence Spec

- (1) **Plist Permission Strings***
- (2) **Framework Imports***
- (3) **Class Instantiations***
- (4) **Authorization Methods***
- (5) **Entitlements***

* Plist used by 1st and 3rd parties.
* Must be all in 1st party files for 1st party practices and in 3rd party files for 3rd party practices. But (6) Additional Evidence suffices in 3rd party files if an Authorization Method is in 1st party files (and vice versa).

B. Signature Detection in App and Library Files

```
1 import UIKit
2 import CoreLocation
3 import HealthKit
4 import HomeKit
5
6 class WorkoutViewController: UIViewController, CLLocationManagerDelegate,
7
8 @IBOutlet weak var gymDistance: UILabel!
9 @IBOutlet weak var recommendedGym: UILabel!
10 @IBOutlet weak var workoutTable: UITableView!
11 var workout = [String]()
12
13 let locationManager = CLLocationManager()
14 let healthKitStore = HKHealthStore()
15
16 let homeManager = HMHomeManager()
17 var homes: [HMHome] = []
18
19 override func viewDidLoad() {
20     super.viewDidLoad()
21
22     workoutTable.backgroundColor = UIColor.lightGray
23     workoutTable.separatorColor = UIColor.blue
24
25     self.locationManager.requestAlwaysAuthorization()
```

Privacy Policy for the Workout With Friends App

Last updated: 05/02/2020
Previous [versions](#)

We are the developers of Workout With Friends. This privacy policy describes how we process your personal information and which privacy rights you have when you are using Workout With Friends. Please contact us at the contact information [below](#) if you have any questions or comments.

- 1. [Personal Information Collection and Use](#)
- 2. [Personal Information Sharing](#)
- 3. [Tracking Technologies](#)
- 4. [Social Logins](#)
- 5. [In-app Purchase Information](#)
- 6. [Children's Personal Information](#)
- 7. [How Long We Keep Your Personal Information](#)
- 8. [How We Protect Your Personal Information](#)
- 9. [Policy Changes](#)
- 10. [Accessibility](#)
- 11. [Contact Us](#)

C. Privacy Policy Generation

1. Personal Information Collection and Use

If you grant Workout With Friends permission, we may collect and use personal information from you as follows.

- **Location Services**
Purpose: We are using your location to recommend a gym nearby.

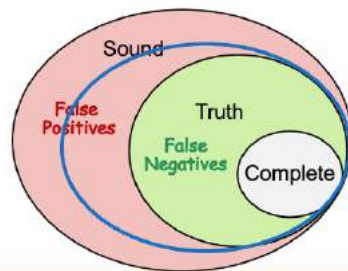
Take-home Messages

1. With the development of deep learning-based NLP (e.g., Transformers, GPTs), more researchers choose to embrace rule-based/pattern matching NLP methods.
2. Accurate mobile app behaviour extraction (Static Analysis + Dynamic Analysis) is challenging!
3. Current studies commonly focus on data entities alignment, neglecting the fine-grained data purposes.

No. Privacy policies	50	No. Privacy policies	50
No. Segments	3,940	No. Segments	7,357
No. Words	103,860	No. Words	194,974
Avg. Segments	79	Avg. Segments	147
Avg. Words	2,120	Avg. Words	3,979

2020

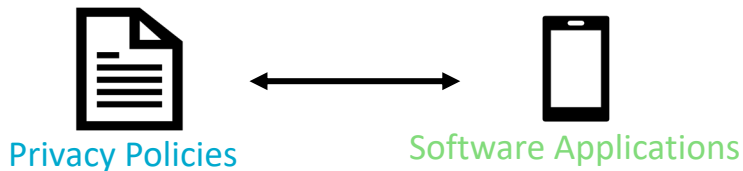
2023



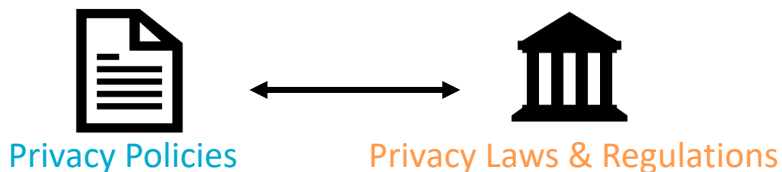
Rice's Theorem

Privacy Policy Research Landscape

1. Content Analysis (PP Descriptions - Software Behaviours):



2. Compliance Checking (PP Descriptions - Law/Reg Requirements)



3. Transparency and Readability of PP and Privacy Notices:

Requirement Extraction from Laws/Regs

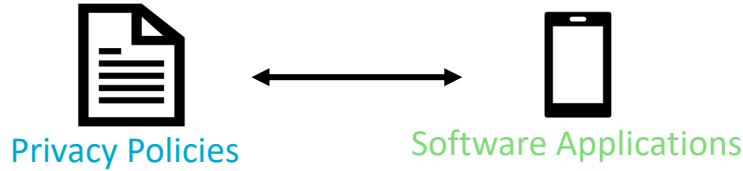
CCPA Requirement	Inubenda	
	May '20	Jan '21
Disclosure of right to request how personal information is collected, used, sold, disclosed for a business purpose, and shared [CCPA §1798.130(a)(5)(A), 1798.110(a), 1798.115(a), Regs §999.308(c)(1)(a)]	✓	✓
Disclosure of right to request deletion of personal information [CCPA §1798.105(b), 1798.130(a)(5)(A), Regs §999.308(c)(2)(a)]	✓	✓
Disclosure of whether personal information is sold and right to opt-out of sale [Regs §999.308(c)(3)(a), 999.308(c)(3)(b), 999.306]	✓	✓
Disclosure of right to not be discriminated against when requesting any rights [CCPA §1798.130(a)(5)(A), 1798.125(a), Regs §999.308(c)(4)(a)]	✗	✗
Instructions for submitting requests and link to online form or portal if offered [Regs §999.308(c)(1)(b), 999.308(c)(2)(b), 999.308(c)(2)(c)]	✓	✓
Instructions for authorized agents to make requests [Regs §999.308(c)(5)(a)]	✓	✓
Description of the process used to verify requests [Regs §999.308(c)(1)(c)]	✓	✓
List of categories of personal information collected in preceding 12 months [CCPA §1798.130(a)(5)(B), 1798.110(c), Regs §999.308(c)(1)(d)]	✓	✓
List of categories of personal information sold in preceding 12 months [CCPA §1798.130(a)(5)(C), 1798.115(c)(1), Regs §999.308(c)(1)(g)(1)]	✓	✓
List of categories of personal information disclosed for business purpose in preceding 12 months [CCPA §1798.130(a)(5)(C), 1798.115(c)(2), Regs §999.308(c)(1)(g)(1)]	✗	✗
For each personal information category, categories of third parties to whom information was disclosed or sold [Regs §999.308(c)(1)(g)(2)]	✓	✓
Categories of sources from which personal information is collected [Regs §999.308(c)(1)(e)]	✓	✓
Business or commercial purpose for collecting or selling personal information [Regs §999.308(c)(1)(f)]	✓	✓
Whether the business has actual knowledge that it sells personal information of minors under 16 years of age and special process [Regs §999.308(c)(1)(g)(3), 999.308(c)(9)]	✓	✓
Contact information for questions or concerns [Regs §999.308(c)(6)(a)]	✓	✓
Date policy was last updated [Regs §999.308(c)(7)]	✓	✓
Special requirements for businesses buying, receiving, selling, or sharing personal information of 10,000,000 or more consumers in a calendar year [Regs §999.308(c)(8), 999.317(g)(1)]	✗	✗
For online notices, follow generally recognized industry standards, such as the W3C Web Content Accessibility Guidelines, version 2.1 of June 5, 2018 [Regs §999.308(a)(2)(d)]	✗	✗

TABLE II: CCPA privacy policy requirements and generators' compliance.

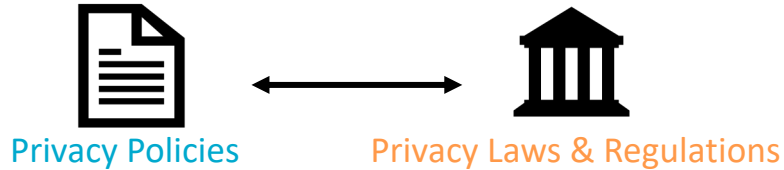
- (1) *Collect Personal Information*: Collect data subjects' information which can identify their personal IDs. [GDPR Art 13.1]
- (2) *Data Retention Period*: Retention period of personal information. [GDPR Art 13.2(a)]
- (3) *Data Processing Purposes*: The purposes of processing personal data. [GDPR Art 13.1(c)]
- (4) *Contact Details*: The contact details of the controller or the Data Protection Officer. [GDPR Art 13.1(a)(b)]
- (5) *Right to Access*: The right (of the data subject) to request from the controller to access their personal information. [GDPR Art 13.2(b)]
- (6) *Right to Rectify or Erase*: The right (of the data subject) to request from the controller to rectify or erase of their personal information. [GDPR Art 13.2(b)]
- (7) *Right to Restrict of Processing*: The right (of the data subject) to request from the controller to restrict processing concerning the data subject. [GDPR Art 13.2(b)]
- (8) *Right to Object to Processing*: The right (of the data subject) to request from the controller to object to processing. [GDPR Art 13.2(b)]
- (9) *Right to Data Portability*: The right (of the data subject) to receive and transmit his/her personal data to another controller. [GDPR Art 13.2(b)]
- (10) *Right to Lodge a Complaint*: The right (of the data subject) to lodge a complaint with a supervisory authority. [GDPR Art 13.2(d)]

Privacy Policy Research Landscape

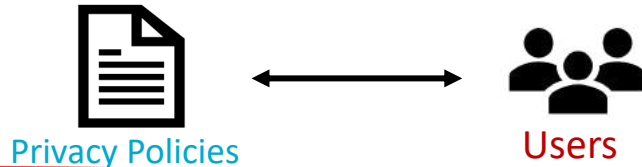
1. Content Analysis (PP Descriptions - Software Behaviours):



2. Compliance Checking (PP Descriptions - Law/Reg Requirements)



3. Transparency and Readability of PP and Privacy Notices:



Motivation: transparent and readability of PPs

1. Requirements in laws/regulations

1. EU General Data Protection Regulations (GDPR)
2. California Consumer Privacy Act of 2018 (CCPA)
3. Australian Privacy Principles (APP): have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information.

2. Users' and consumers' practical need

According to a survey conducted by The Washington Times, 36% of interviewees **never** read privacy policies, and 38% of interviewees sometimes read privacy policies.

Development History

1. Privacy Policy



2. Privacy Icons

DaPIS: The Data Protection Icon Set



3. Platform for Privacy Preference

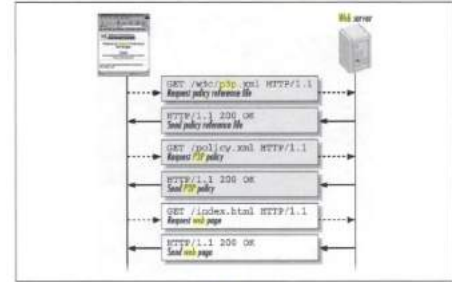


Figure 1-1. The basic protocol for fetching a P3P policy

4. Privacy Labels



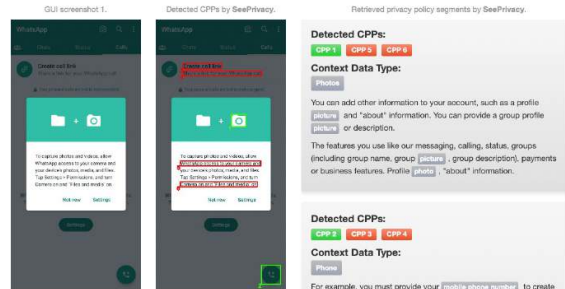
5. Contextual Privacy Policy



Example 1: WhatsApp

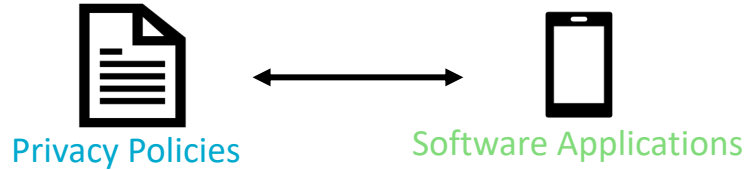
There are two inputs of SeePrivacy to generate CPP for a mobile app:

1. WhatsApp's [privacy policy](#) in HTML format;
2. The current GUI screenshot that you would like to generate CPP (the leftmost).

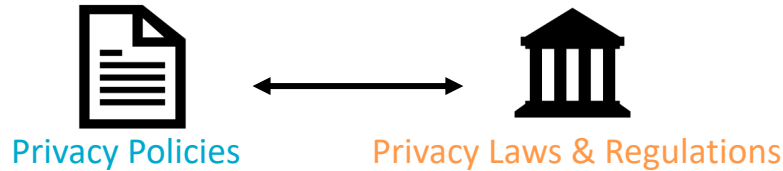


Privacy Policy Research Landscape: My research

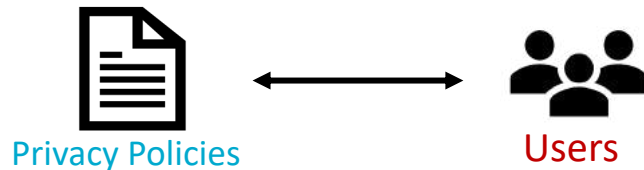
1. Content Analysis (PP Descriptions - Software Behaviours):



2. Compliance Checking (PP Descriptions - Law/Reg Requirements)



3. Transparency and Readability of PP and Privacy Notices:



An Empirical Study of Automated {Privacy Policy Generators}

[Topic]: Content Analysis + Compliance Analysis

[Venue]: USNEIX Security 2024

Is It a Trap? A Large-scale Empirical Study And Comprehensive Assessment of Online Automated Privacy Policy Generators for Mobile Apps

Shidong Pan^{*} Dawen Zhang Mark Staples
CSIRO's Data61 & ANU CSIRO's Data61 & ANU CSIRO's Data61
Zhenchang Xing Fieshan Chen Xiwei Xu Thong Hoang[†]
CSIRO's Data61 & ANU CSIRO's Data61 CSIRO's Data61 CSIRO's Data61

{Contextual Privacy Policy} for Mobile Apps

[Topic]: Transparency and Readability of Privacy Policies

[Venue]: USNEIX Security 2024

A NEW HOPE: Contextual Privacy Policies for Mobile Applications and An Approach Toward Automated Generation

Shidong Pan^{1,2†}, Zhen Tao^{1,2}, Thong Hoang^{2†}, Dawen Zhang^{1,2}, Tianshi Li³, Zhenchang Xing^{1,2}, Xiwei Xu², Mark Staples², Thierry Rakotoarivelo², and David Lo⁴

¹School of Computing, Australian National University

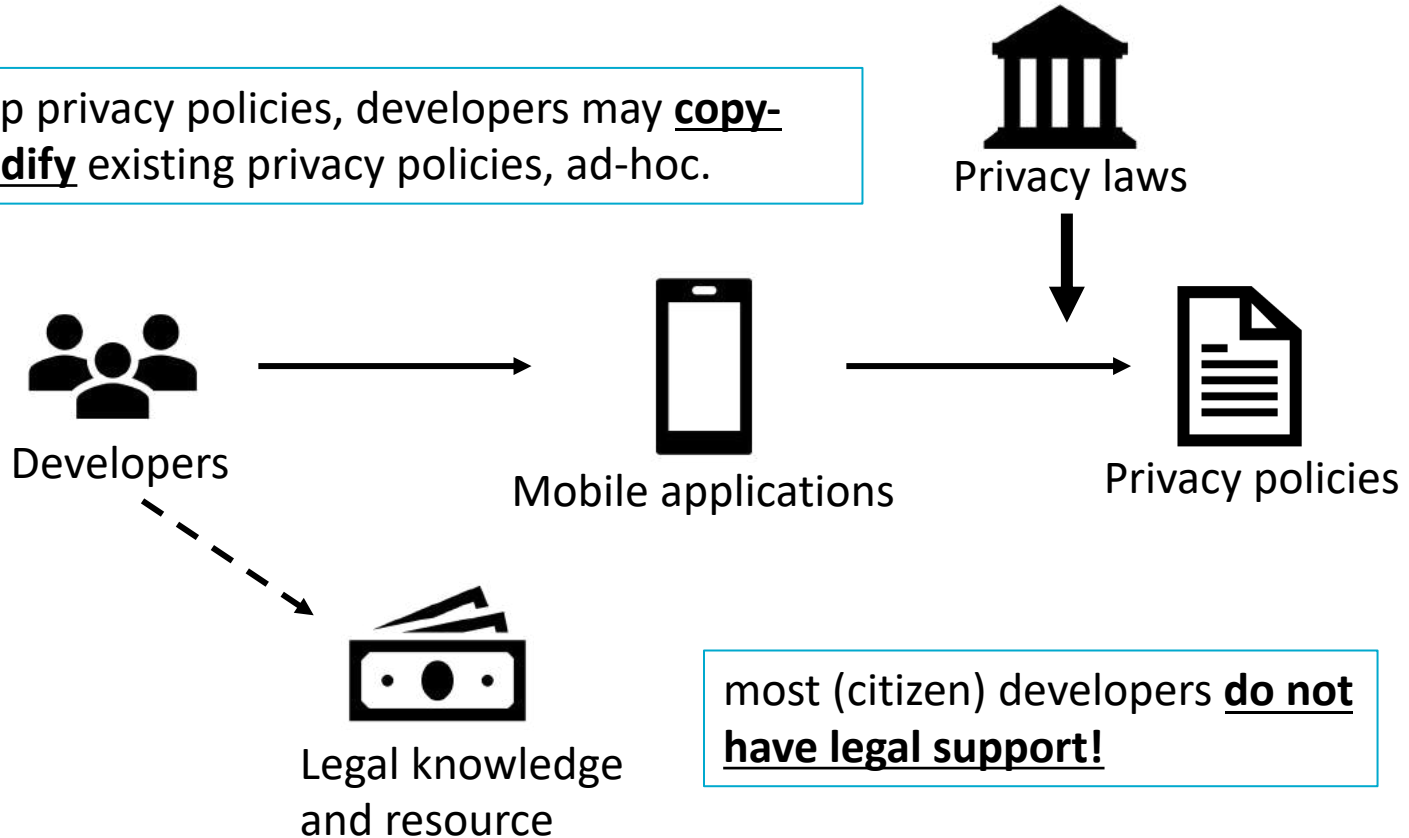
²Software and Computational Systems Research Program, CSIRO's Data61

³Khoury College of Computer Sciences, Northeastern University


⁴School of Computing and Information Systems, Singapore Management University

How do those problematic privacy policies be crafted?

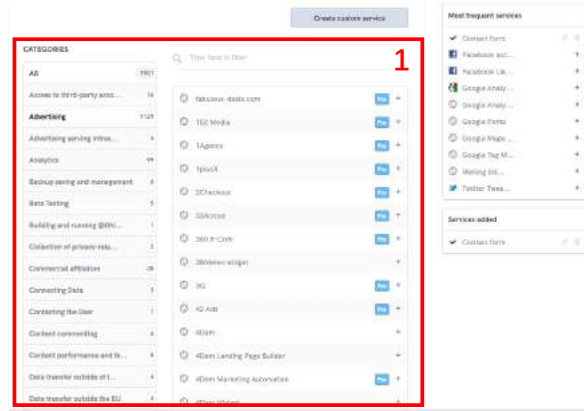
To develop privacy policies, developers may **copy-paste-modify** existing privacy policies, ad-hoc.



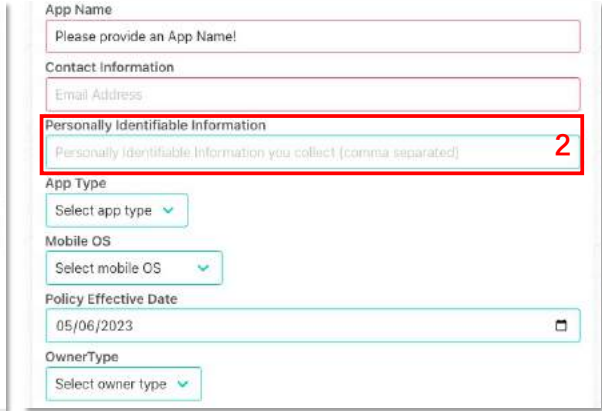
Online Automated Privacy Policy Generator (APPG) as the Solution

 Online **Automated Privacy Policy Generators** can provide more automated and systematic solutions for developers, rather than through ad-hoc copy-paste-modify.

However, their **quality and other characteristics** can vary and are not yet deeply understood.



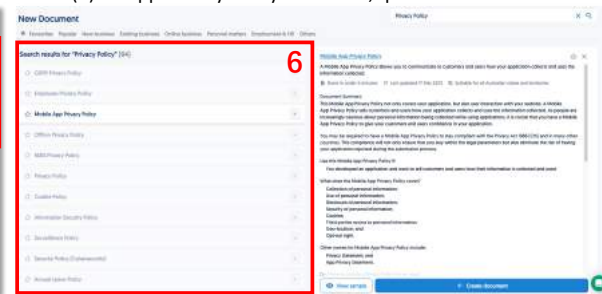
(a) #1 lubenda, UI-mode



(b) #2 App Privacy Policy Generator, questionnaire-mode



(c) #3 Termly, questionnaire-mode



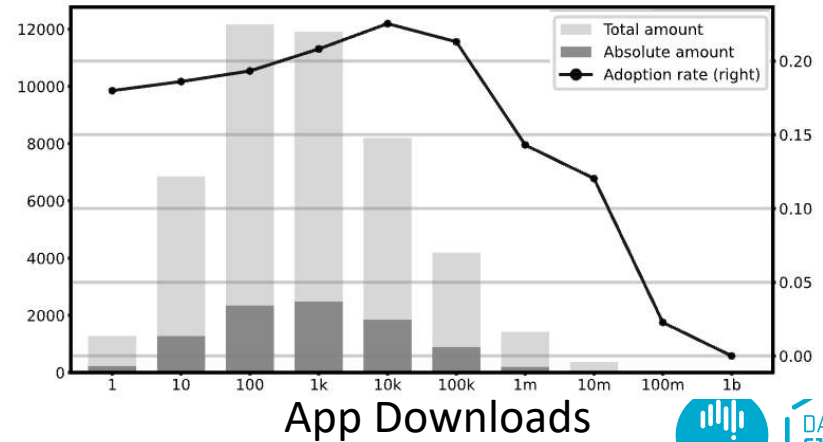
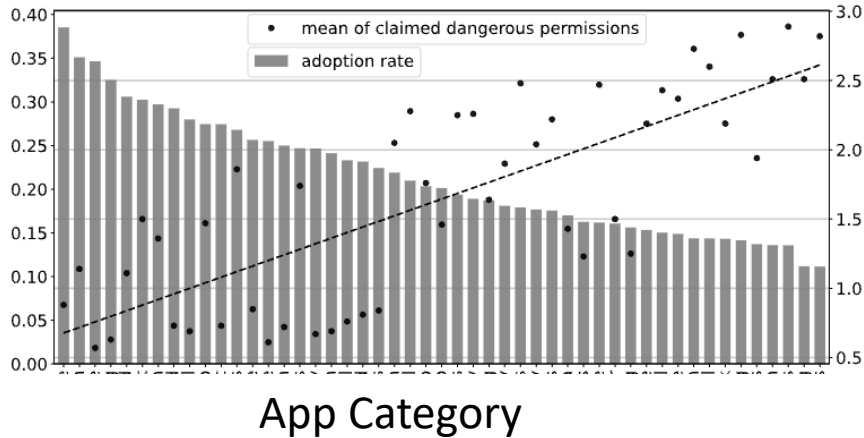
(d) #10 Lawpath, document-mode

The Prevalence of APPGs in Market

Table 4: Summary of market use of different APPGs.

Method	Market Occupancy
Fingerprint Keyword Searching	6.6% (3,066)
Document Similarity Comparison	18.1% (8,425)
Intersection	4.4% (2,042)
Union (Total)	20.1% (9,332)

The market occupancy ratio of 10 examined APPGs is around **20.1%**!



The Compliance of APPGs against Regulations

Table 6: Tallies of the APPGs' compliance against legal requirements in privacy regulations. The individual requirements of LGPD are shown in Table 5. "N.R." stands for "no record". The enforcement date of LGPD is September 2020.

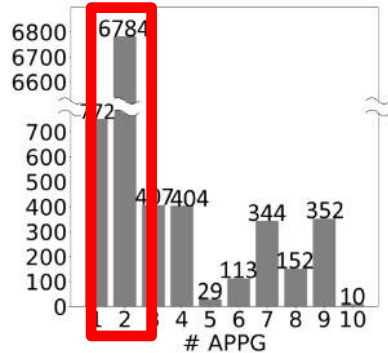
#	GDPR			CCPA			LGPD
	May'20	Jan'21	May'22	May'20	Jan'21	May'22	May'22
1	8/8	8/8	8/8	14/18	14/18	14/18	8/8
2	N.R.	N.R.	3/8	N.R.	N.R.	3/18	3/8
3	8/8	8/8	8/8	3/18	15/18	15/18	6/8
4	8/8	8/8	8/8	5/18	16/18	16/18	6/8
5	N.R.	N.R.	0/8	N.R.	N.R.	2/18	1/8
6	N.R.	N.R.	0/8	N.R.	N.R.	2/18	1/8
7	8/8	8/8	8/8	5/18	16/18	16/18	6/8
8	N.R.	N.R.	8/8	N.R.	N.R.	11/18	5/8
9	8/8	8/8	8/8	5/18	16/18	16/18	6/8
10	N.R.	N.R.	2/8	N.R.	N.R.	2/18	4/8

Table 7: The disclosure existence of seven fundamental data rights. Numbers in the first row indicate APPGs as per Table 1, and "Apps" denotes the tallies of disclosure for 12 leading apps.

Data Right	1	2	3	4	5	6	7	8	9	10	Apps
Right to Know	X	X	✓	X	X	✓	✓	✓	✓	✓	12/12
Right to Access	X	X	✓	X	X	✓	✓	✓	✓	✓	12/12
Right to Processing	X	X	✓	X	X	✓	✓	✓	X	✓	12/12
Right to Restrict of Processing	X	X	✓	X	X	✓	✓	✓	X	✓	12/12
Right to be Forgotten	X	X	✓	X	X	✓	✓	✓	✓	✓	12/12
Right to Data Transfer	X	X	✓	X	X	✓	✓	✓	X	✓	12/12
Right to Lodge a Complaint	X	X	✓	X	X	✓	✓	✓	✓	✓	12/12

Table 8: The disclosure existence of five highly concerning privacy practices. Numbers in the first row indicate APPGs as per Table 1, and "Apps" denotes the tallies of disclosure for 12 leading apps.

Privacy Practice	1	2	3	4	5	6	7	8	9	10	Apps
Data Encryption	✓	✓	✓	✓	X	X	✓	✓	✓	✓	8/12
Government Requests	✓	X	✓	X	X	X	✓	✓	✓	X	11/12
Data Breach Notification	X	X	X	X	X	X	✓	X	X	✓	1/12
Changes Notification	✓	X	✓	X	X	✓	✓	✓	✓	X	12/12



The #2 App Privacy Policy Generator is the most popular one, boasting a 72.7% adoption rate. Users tend to select easy-to-use APPGs even though at the cost of a potentially-higher risk to breach privacy regulations.

Implications and Findings to Stakeholders



- **App developers/APPG users:** While app developers may benefit from using APPGs to create privacy policies more efficiently, they should be aware of APPGs' latent limitations.



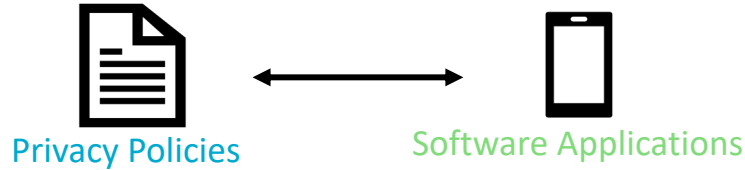
- **APPG providers:** Our analysis suggests APPG providers should work on improving recognised data use, since the majority of APPGs on the market only provide a very limited scope of personal information and device permissions.



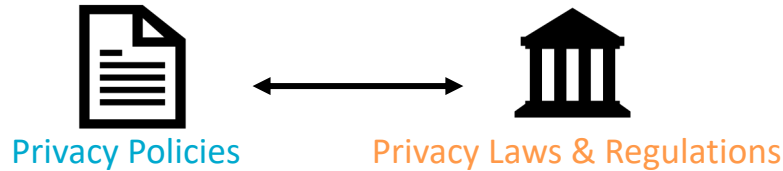
- **Privacy regulators:** Regulators should recognize the importance of this issue and be engage with this emerging market trend.

Privacy Policy Research Landscape: My research

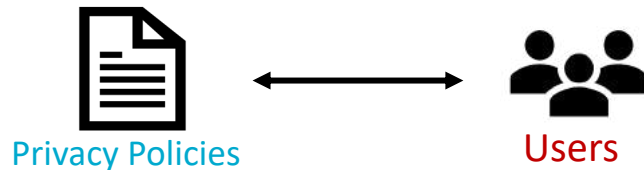
1. Content Analysis (PP Descriptions - Software Behaviours):



2. Compliance Checking (PP Descriptions - Law/Reg Requirements)



3. Transparency and Readability of PP and Privacy Notices:



An Empirical Study of Automated {Privacy Policy Generators}

[Topic]: Content Analysis + Compliance Analysis

[Venue]: USNEIX Security 2024

Is It a Trap? A Large-scale Empirical Study And Comprehensive Assessment of Online Automated Privacy Policy Generators for Mobile Apps

Shidong Pan^{*} Dawen Zhang Mark Staples
CSIRO's Data61 & ANU CSIRO's Data61 & ANU CSIRO's Data61
Zhenchang Xing Fieshan Chen Xiwei Xu Thong Hoang[†]
CSIRO's Data61 & ANU CSIRO's Data61 CSIRO's Data61 CSIRO's Data61

{Contextual Privacy Policy} for Mobile Apps

[Topic]: Transparency and Readability of Privacy Policies

[Venue]: USNEIX Security 2024

A NEW HOPE: Contextual Privacy Policies for Mobile Applications and An Approach Toward Automated Generation

Shidong Pan^{1,2†}, Zhen Tao^{1,2}, Thong Hoang^{2†}, Dawen Zhang^{1,2}, Tianshi Li³, Zhenchang Xing^{1,2}, Xiwei Xu², Mark Staples², Thierry Rakotoarivelo², and David Lo⁴

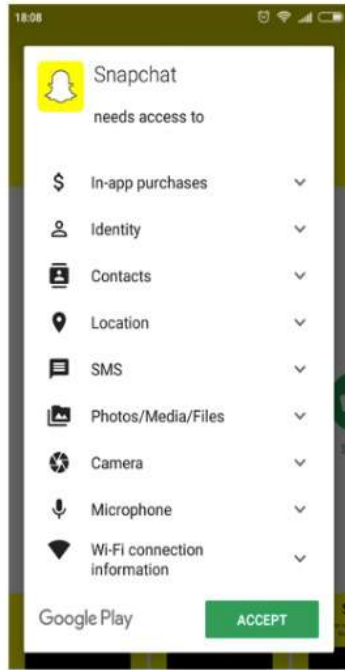
¹School of Computing, Australian National University

²Software and Computational Systems Research Program, CSIRO's Data61

³Khoury College of Computer Sciences, Northeastern University

⁴School of Computing and Information Systems, Singapore Management University

Development of “Just-in-time” Privacy Notices



(a) Install-time



(b) Invoke-time



(c) Context-aware

Android 6.0

Contextual Privacy Policy for Mobile Apps



Example 1: WhatsApp

There are two inputs of SeePrivacy to generate CPP for a mobile app:

1. WhatsApp's [privacy policy](#) in HTML format;
2. The current GUI screenshot that you would like to generate CPP (the leftmost).

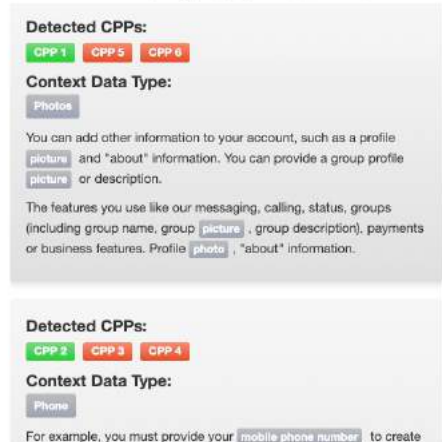
GUI screenshot 1.



Detected CPPs by SeePrivacy.

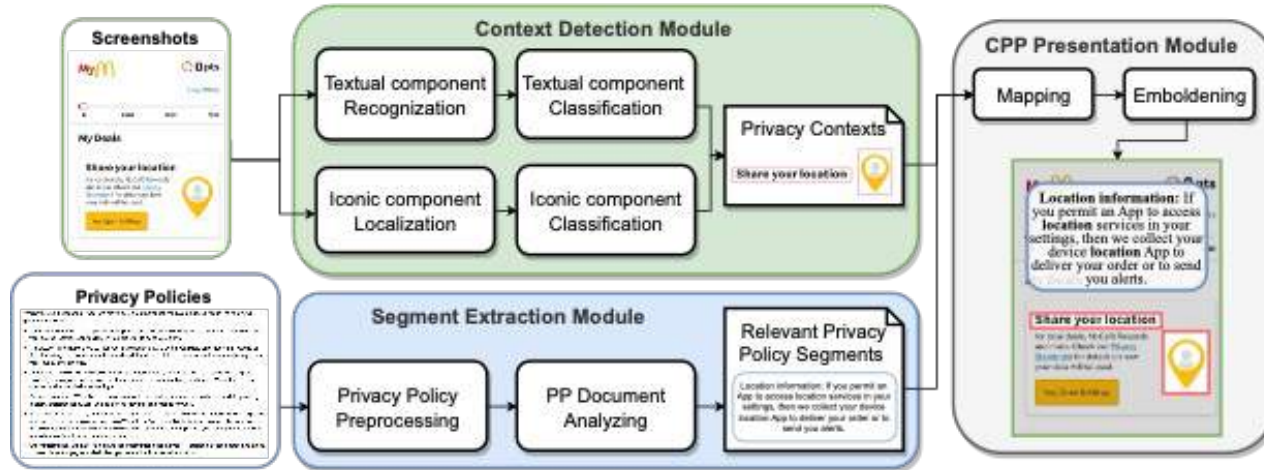


Retrieved privacy policy segments by SeePrivacy.



- The aim of **Contextual Privacy Policy** is to fragment **privacy policies** into concise **snippets**, displaying them only within the corresponding contexts within the application's **graphical user interfaces** (GUIs).

Contextual Privacy Policy for Mobile Applications



Our multi-modal framework synergistically combines Computer Vision (CV) techniques, pre-trained Large Language Model (LLMs), and Natural Language Processing (NLP) techniques.

An Adoption Scenario: CPP in Market

LINE: Calls & Messages ¹

LINE Corporation
Contains ads - In-app purchases ²

3.8★ 500M+ Downloads
13.8M reviews Rated for 3+ ³

Install Share Add to

Beyond texting ⁵
Chat with friends 1-on-1 or in groups.
If you do not provide certain types of information such as your phone number which needs to be registered for using our Services, you may not be able to use all or a part of our Services.

Exciting stickers
Express yourself with fun stickers and create sharing packs.

Stay in the know
Discover points and rewards that will keep you in the know.

App support ⁴

- Website
- Support email: line-support@line.me
- Address: 東京都新宿区四谷一丁目6番1号

Privacy Policy

More by LINE Corporation

We will not in any way use highly private information such as texts, images, videos and audio data sent in a talk room between users.

Implications and Broader Impacts


SeePrivacy About Examples Demo PET Contact

What is SeePrivacy?

Privacy policies have become the most critical approach to safeguarding individuals' privacy and digital security. To enhance their presentation and readability, the concept of **Contextual Privacy Policies (CPPs)** was gradually developed, aiming to fragment policies into shorter snippets and display them only in corresponding contexts.

We are the first to propose a novel multi-modal framework, namely **SeePrivacy**, designed to automatically generate contextual privacy policies for mobile apps.

Our framework does **not** require the access to apps' source code or Android APIs; hence, the framework can be easily deployed with lower security concerns.



What can SeePrivacy bring to you?



Privacy notice

SeePrivacy aims to protect personal



Just-in-time reminder

Privacy notices are closely and timely.



Readability

SeePrivacy enhances the presentation



Comprehensibility

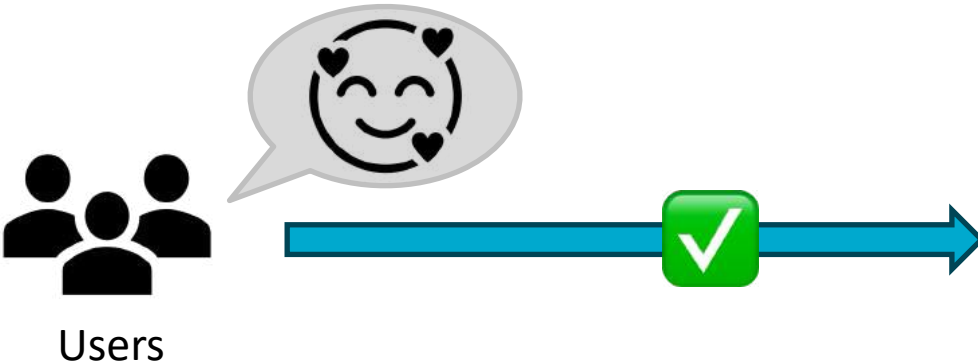
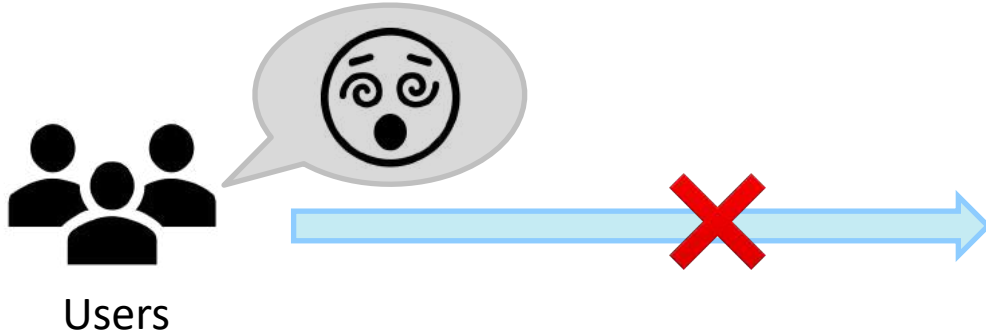
SeePrivacy effectively assists users in

These findings suggest that our framework could serve as a significant tool for **bolstering user interaction with, and understanding of, privacy policies**. Furthermore, our solution has the potential to make privacy notices more **accessible** and **inclusive**, thus appealing to a broader demographic.

Showcase website: <https://cpp4app.github.io/>

Live demo: <https://huggingface.co/Cpp4App/>

User-Centric Privacy Enhancing Toolkit (U-PET)



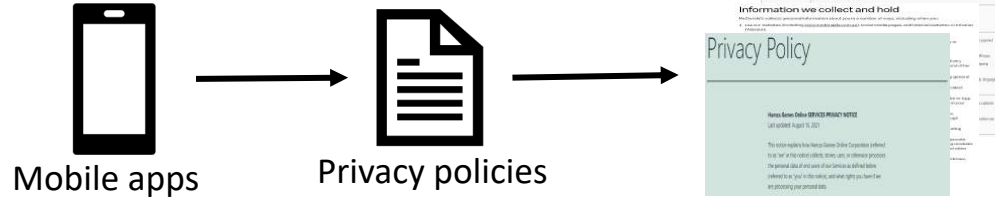
Privacy Information



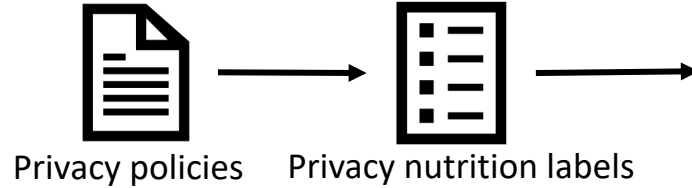
Transparent and Engaging Privacy Information



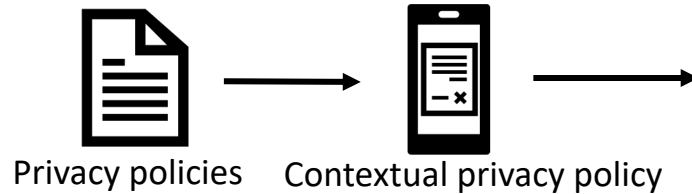
1. Automated Privacy Policy Generators (APPGs)



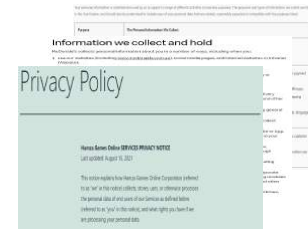
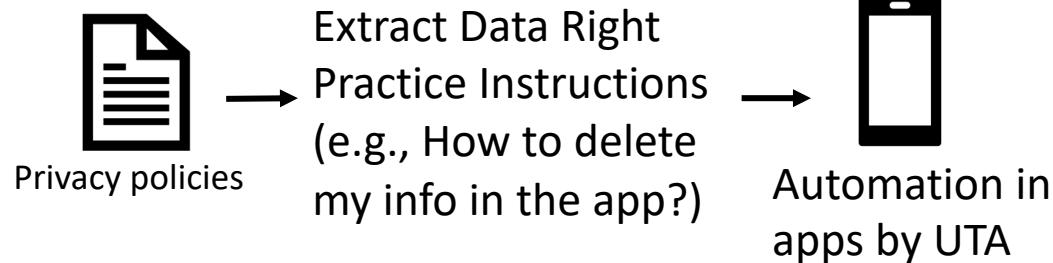
2. Privacy Nutrition Labels From Privacy Policies (Policy2Label)



3. Contextual Privacy Policy for Mobile Apps (Cpp4App)



4. Data Rights Extraction and Automation in Mobile Apps (AutoYourRight)





Australia's National Science Agency

{Privacy Policy} in Practice: Challenges, Implications, and Solutions

Hope you enjoy the content :)

Shidong.Pan@anu.edu.au

University of Edinburgh

March 2024