

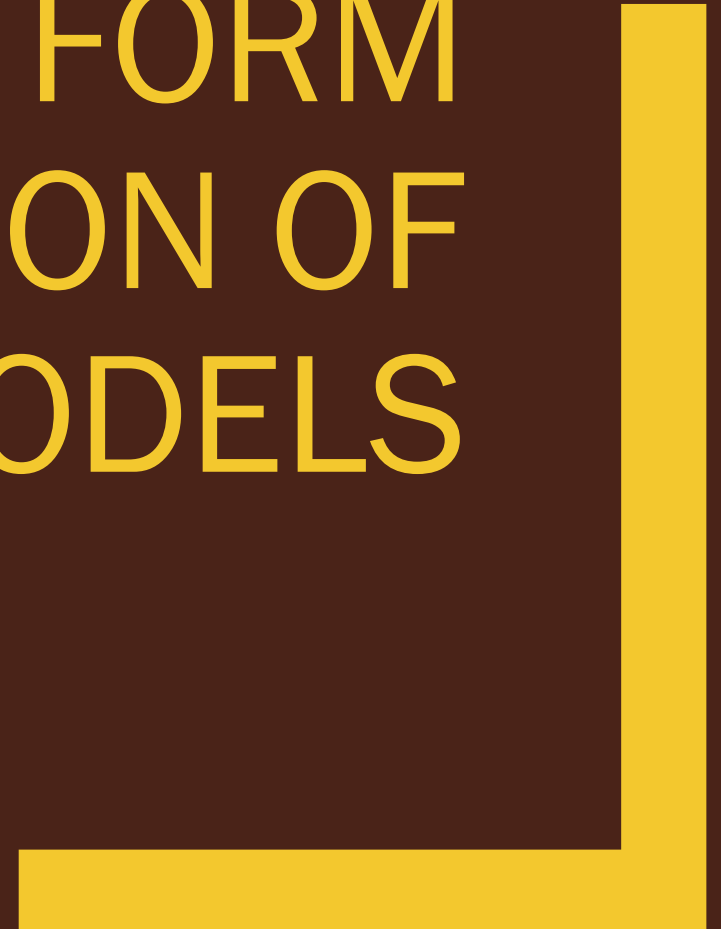
# CROSS-PLATFORM COMPARISON OF PERMISSION MODELS

Maryam Mehrnezhad

Royal Holloway University of London, UK

[Maryam.mehrnezhad@rhul.ac.uk](mailto:Maryam.mehrnezhad@rhul.ac.uk)

W3C Permission Workshop 2022



Part I:

Cross-platform Analysis of Online  
Tracking (PC browser, Mobile browser,  
Mobile App)

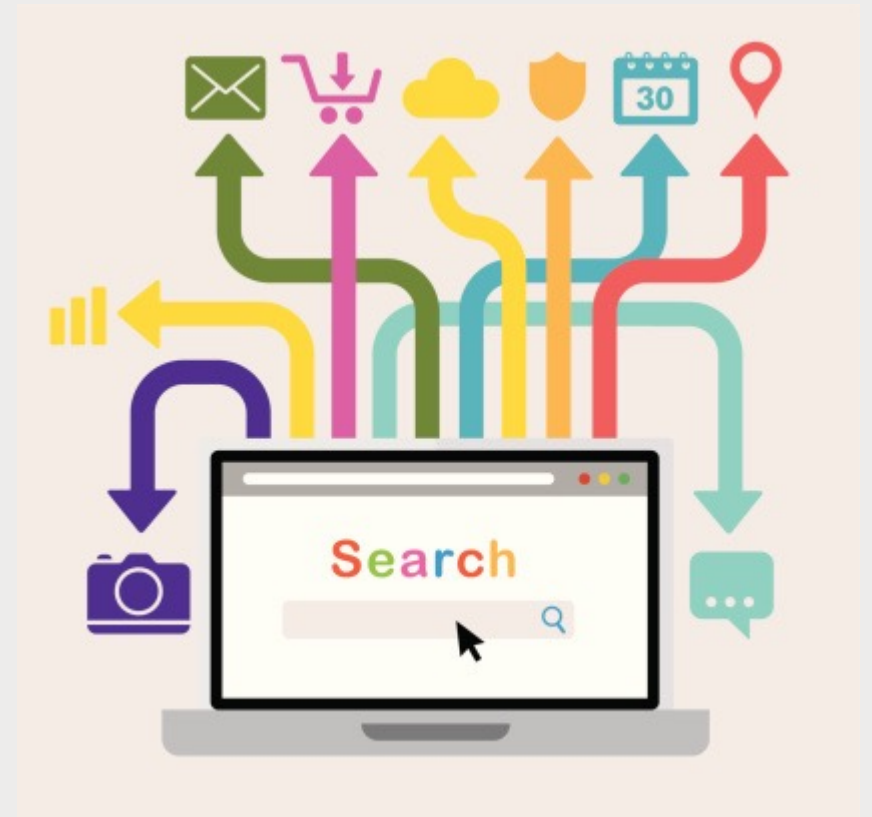
# A CROSS-PLATFORM EVALUATION OF USER ONLINE PRIVACY

Maryam Mehrnezhad

Paper at The European Symposium on Usable Security  
(EuroUSEC) 2020

# Online Tracking

- *Online tracking is collecting data about users online to gain **insight** into users, their behaviour and preferences.*
- *Powerful tools for optimising user experience, statistical purposes, **profiling and targeted marketing**.*
- *It is **not clear** to users when, how, and by whom they are being tracked.*
- *Tracking happens via IP addresses, **cookies**, devices and browser **fingerprinting***
- *On **all platforms**: desktop computers, mobile devices and IoT devices.*



# General Data Protection Regulations (GDPR)



- GDPR is a regulation on data protection and privacy in the **EU** and for the European **citizens** around the globe, came into full affect in May **2018**
- **Consumers** are granted more rights in **controlling** their own information, including the right of **not giving** any personal data to businesses
- Businesses are allowed to collect and process personal data only if consumers **consent** to the term
- Failure to comply results in an enormous **fine** of up to €20 million
- Other privacy laws: California Consumer Privacy Act (CCPA), Chinese Personal Information Security Specification (PISS), Indian Personal Data Protection Bill (PDP Bill)

# A Cross-platform Study

- **Three platforms:** PC browsers, Mobile Browsers, Mobile Apps
- **Top116 EU websites** (from top 150 websites) and **101 Android apps**
- In April and May 2020 (Lockdown)
- **Evaluation:**
  - *Presentation of **Privacy Notice** (Firefox, Chrome, Brave) and Apps*
  - *User **Control Options** (reject, accept, settings, no notice)*
  - ***Tracking Activities** (before engaging with the notice) (Brave and Lumen)*
  - *Offered **Privacy Enhancing Technologies (PETs)***
- **GDPR Reality Check**

# Privacy Notice Location

- The privacy notices on websites and apps are displayed in **various locations** (top, bottom, middle, full-page) and **ways** (in-line, overlay, new-page) **across services, browsers, and platforms**
- The most **popular designs** found on these websites and apps are **not necessarily the most effective ones** in terms of the likelihood of user **engagement**

Position		PC Browser	Mobile Browser
Bottom	Overall	43%	48%
	Right	5%	1%
	Left	2%	-
Middle	Overlay	22%	11%
	In-page	1%	1%
Top	Overlay	7%	2%
	In-page	11%	8%
Full-page		-	20%
No notice		9%	9%

TABLE 1. PRIVACY NOTICE PRESENTATION IN THE TOP 116 EU WEBSITES, PC VS. MOBILE

Position	Android App
Full-page	16%
Middle	8%
Bottom	7%
Top	1%
No notice	51%
Left behind log-in	17%


TABLE 2. PRIVACY NOTICE PRESENTATION IN 101 ANDROID APPS (OF 116 EU WEBSITES)

6:01

edition.cnn.com

CNN

## Diplomats fear blow to US moral authority




Current and ex-diplomats tell CNN the events at home are 'heartbreaking' -- and undermine their

We use cookies and similar technologies ("cookies") to understand how you use our site and to improve your experience. This includes Personalisation; ad selection, delivery, reporting; measurement; content selection, delivery, reporting; and information storage and access. To accept or manage the use of cookies [click here](#). You may read more about vendors that we use by clicking [Show Vendors](#)

I Accept

6:01



### Some important information about how we use your data

We use your information and data to optimize our service and provide you the best possible news experience.

Please tap Accept and Continue if you agree to allow CNN to use data from your device to analyze and measure how you use the app, to make personalised content recommendations, and to serve more relevant advertising.

If you would like more information about how we use your data, or to review and modify your data settings, please tap Manage Data Settings.

Manage Data Settings

Accept and Continue

An example of inconsistencies in:

- **location,**
- **user options, and**
- **content**

of privacy notice of a website in:

- mobile **browser** (left) vs.
- Its mobile **app** (right)

App notices contain a different terminology -> less use of cookies



# Privacy Notice Control Options

- The user options in cookie consents are **inconsistent across services, browsers, and platforms**
- Where the **majority** of these services **nudge** the user to **accept** the notice
- A practice which is **not-complaint** with the law
- Dark patterns

Category	Default	PC Browser	Mobile Browser
Agree or Reject	No default	3%	3%
	Agree	2%	2%
	Reject	1%	1%
Agree or Settings	No default	8%	8%
	Agree	36%	35%
	In-page options	2%	2%
Only agree		28%	27%
Links		12%	14%
No notice		9%	9%

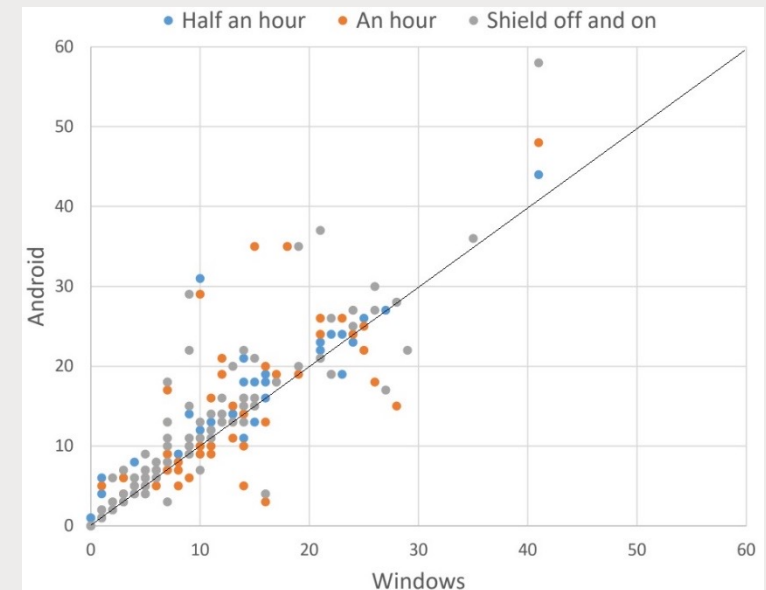
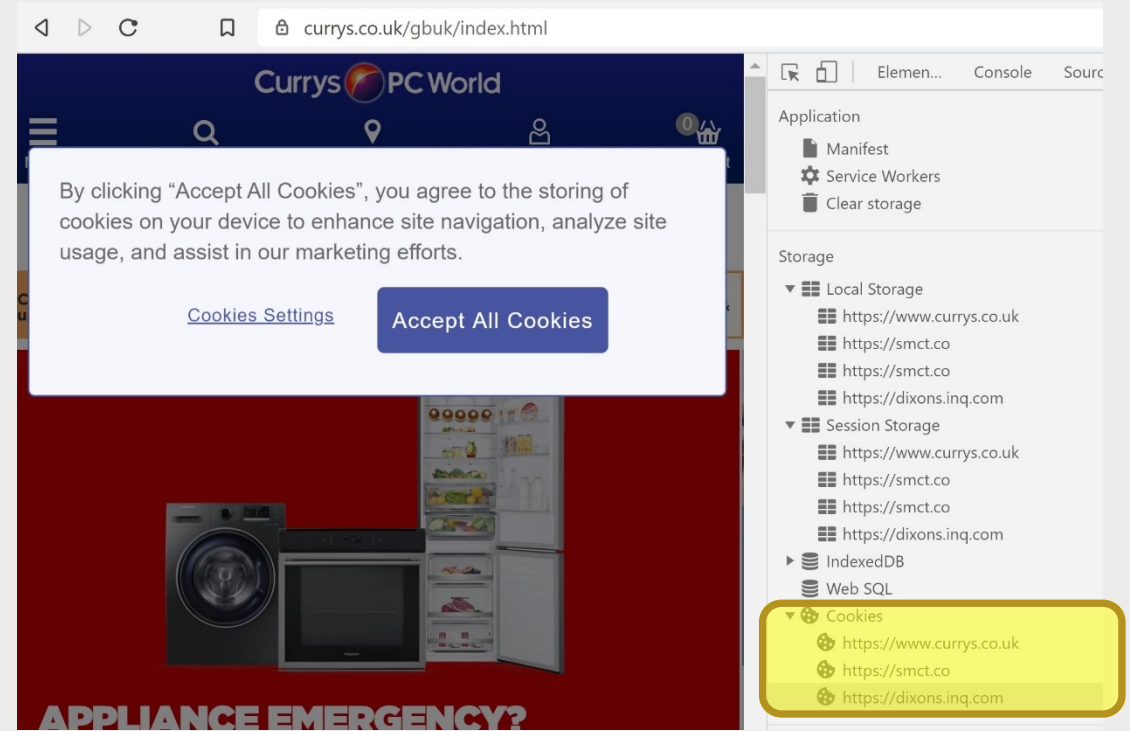
TABLE 3. PRIVACY NOTICE USER CONTROL OPTIONS IN TOP 116 EU WEBSITES, PC VS. MOBILE

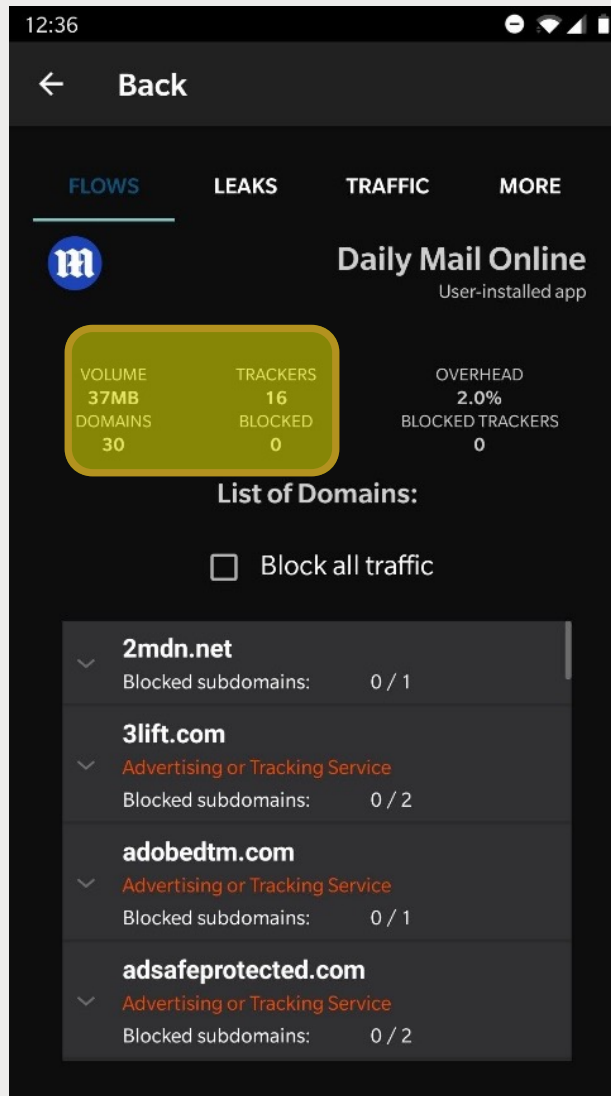
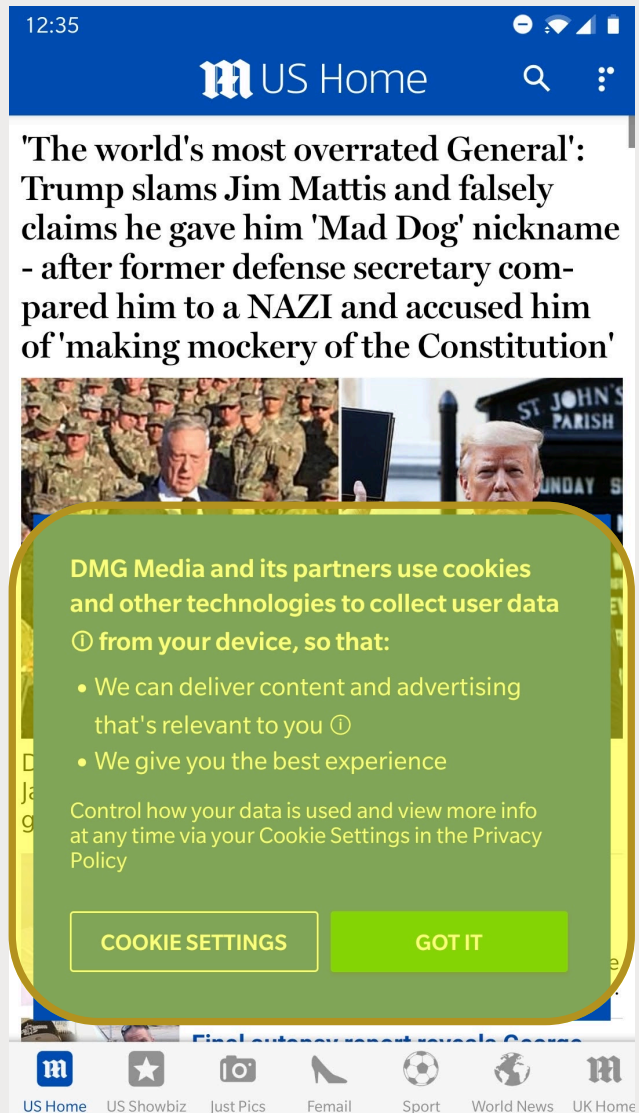
Category	Default	Android App
Agree or Reject	No default	5%
	Agree	2%
	Reject	-
Agree or Settings	No default	2%
	Agree	13%
	In-page options	-
Only agree		8%
Links		2%
No notice		51%
Left behind log-in		17%

TABLE 4. PRIVACY NOTICE USER CONTROL OPTIONS IN 101 CORRESPONDING ANDROID APPS (OF 116 EU WEBSITES)

# Actual Tracking

- Used Brave (privacy-oriented browser) and Lumen (privacy enhancing app)
- The majority of these online services start tracking the user before any interaction with the privacy consent
- Another non-complaint behaviour which was observed in **all platforms**.
- The average tracking activities on Windows were less than Android; **highly correlated**
- The Android app's tracking **moderately correlated**
- Privacy notice can be a **tracker**, and cookies are **placed before** the user interaction





An example of:

- an Android app cookie consent (left) and
- The **identified trackers by Lumen** (right) before any user interaction with the privacy notice.

# Privacy Enhancing Technologies

- Browser Settings (e.g. DNT, deleting cookies manually)
- Browser add-on (e.g. Google Analytics Opt-out Add-on)
- Initiatives (e.g. EDAA, DAA, IAB, NAI, [allaboutcookies.org](http://allaboutcookies.org), [privacysshield.gov](http://privacysshield.gov), and [cookielaaw.org](http://cookielaaw.org))
- Website & account settings (e.g. dashboards, major companies such as fb and google)
- Mobile & app settings
- Privacy-aware browsers (e.g. privacy-oriented browsers)
- Account deactivation
- Contacting service provider
  
- **But, The user has to go way beyond the first page to be able to find and use these**

# Take-away

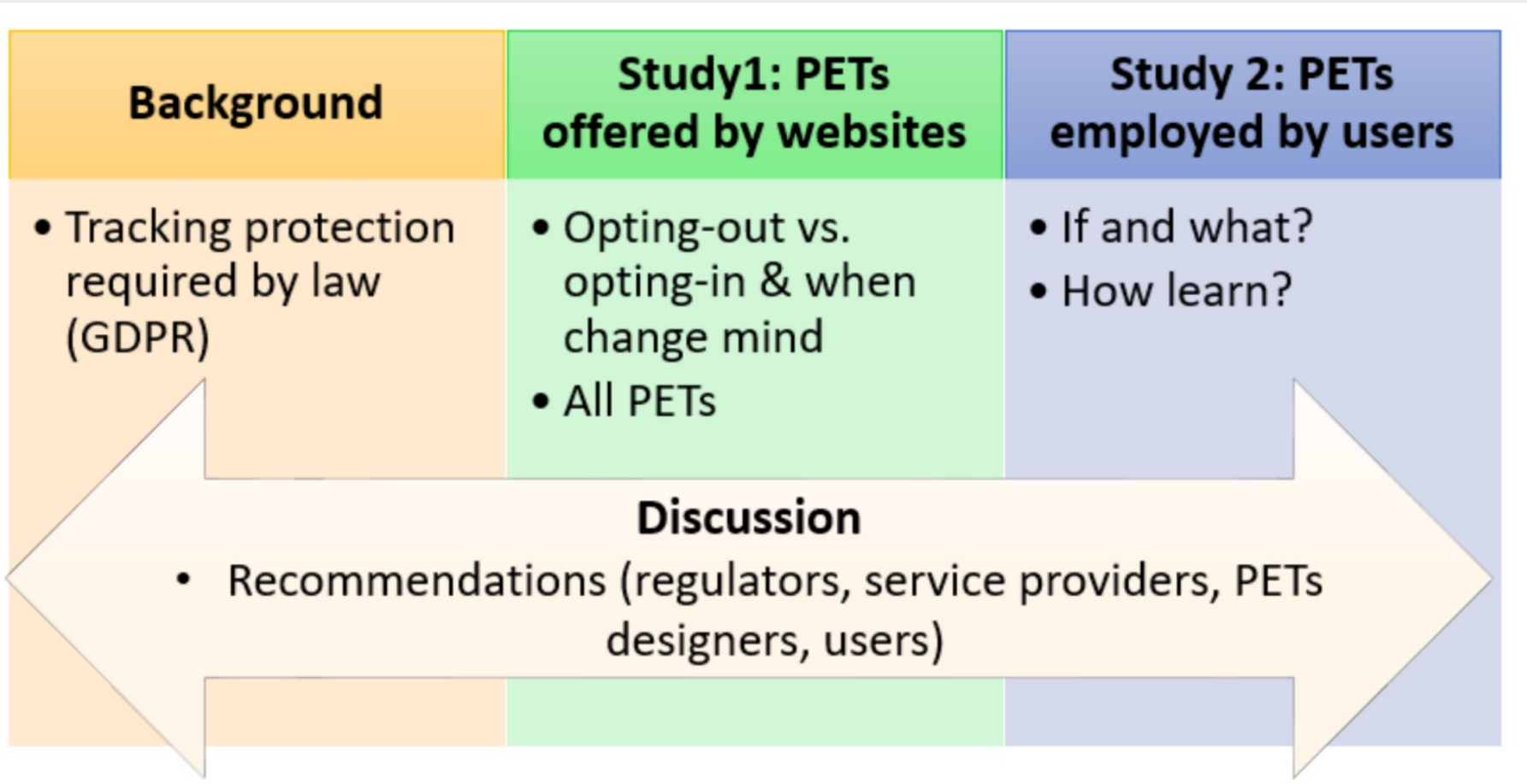
- The privacy **consent** banner and user options are **inconsistent**; most of them are **not complying to the GDPR**
- These services **start tracking** the user once the service (website, app) starts and **before the user's interaction** with notice; another **non-compliant practice** violating user's privacy.
- The tracking behaviours of online services across platforms are **intrusive** and **correlated**.
- Current practices for protecting user online privacy are **not effective** and the blind spots are increasing as online services are being offered on various platforms such as mobile and IoT.
- Users can protect themselves by
  - Use **privacy-oriented** browsers (*Brave, Tor, Private and incognito browsing*)
  - Take their time with the privacy notice and **opt-out** (*frustrating!*)
  - **Uninstall unnecessary apps** from your mobile device
  - **Pay attention to the permissions** they give to services

# **Part II: User Studies and Website Studies**

# HOW CAN AND WOULD PEOPLE PROTECT FROM ONLINE TRACKING?

Maryam Mehrnezhad, Kovila Coopamootoo, Ehsan Toreini

Paper at The 22nd Privacy Enhancing Technologies Symposium  
(PoPETs) 2022



**Fig. 1.** Overall scope of the paper



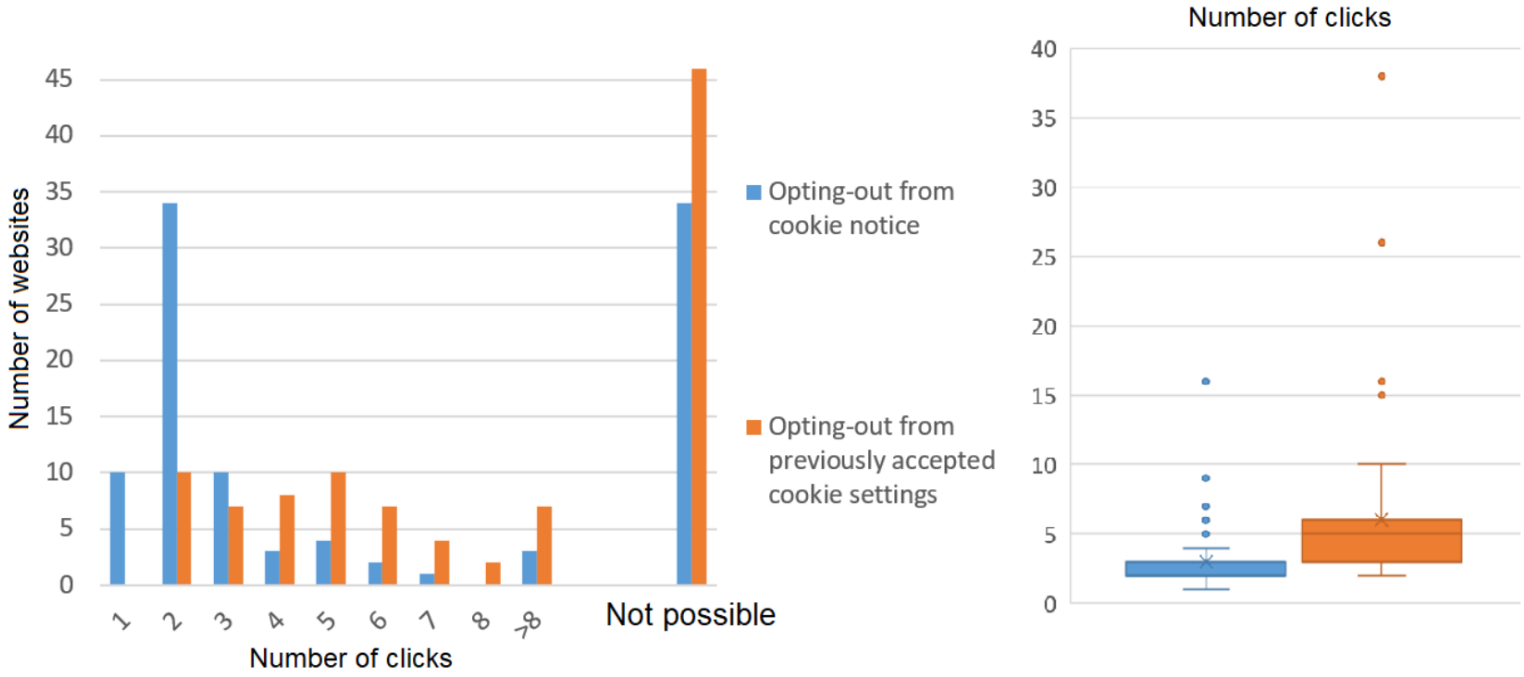
# Part 1- System Study

- RQ1: What are the implications of opting-out of privacy consent and when **user changes mind**?
- RQ2: What are **all sorts of PETs** offered to the user in these websites?
- 100 top EU websites (Alexa)

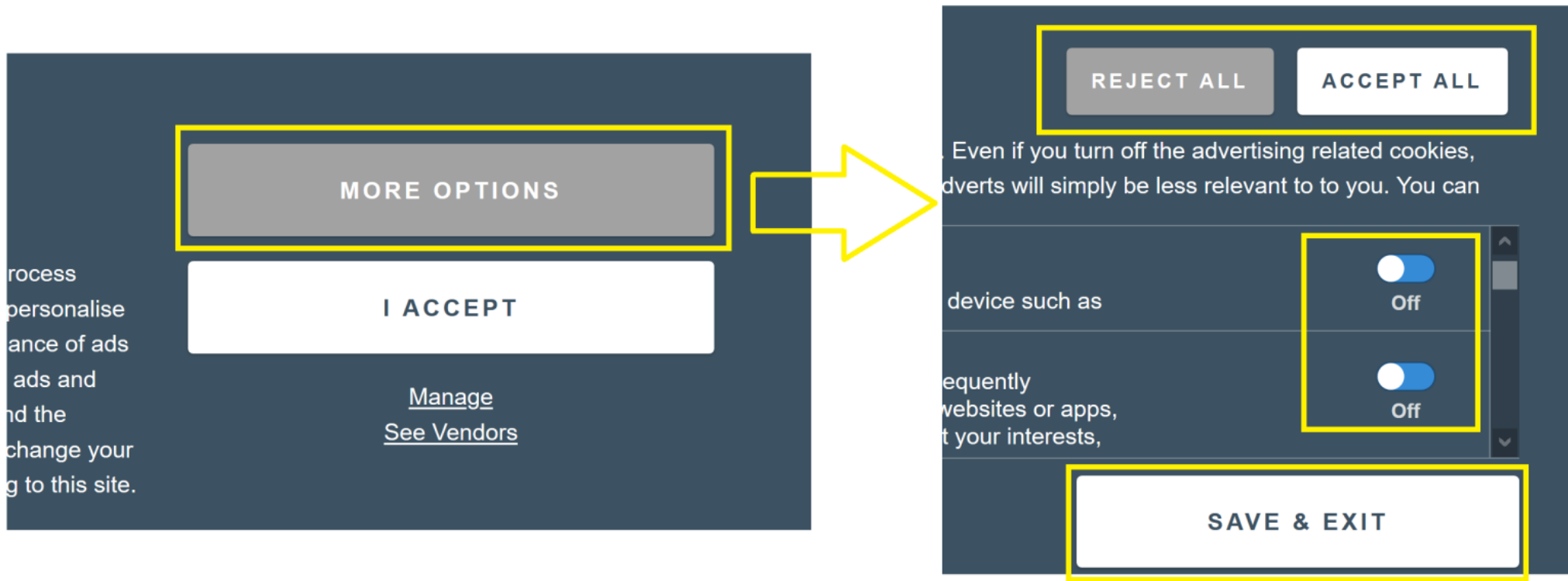
Control options	Other options	no. of websites
None		5
Notification		15
Only Accept		22
Highlighted Accept	Reject	3
	Options	41
Accept	Reject	3
	Options	11

**Table 1.** Cookie notice control options in top 100 EU websites

# Withdrawing a Previously Given Consent



**Fig. 2.** Opting-out when website visited for the first time vs. Opting-out of previously accepted settings, Left: Number of websites for each click count, Right: the distribution of number of clicks. Websites with no opt-out options are excluded from the right plot.



**Fig. 3.** Example of opting-out via cookie notice and existing violations (Accept is highlighted and cookies are pre-selected).

# PETs Offered by Top 100 EU Websites

<b>Category</b>	<b>no. of websites</b>
Contacting service provider	94
Browser settings	90
Initiatives	73
Opting-out of 3rd party websites	66
Information Commissioner's Office (ICO)	53
Website & account settings	34
Browser add-on	25
Mobile & app settings	21

**Table 2.** PETs offered by top 100 EU websites

# Part 2: User Study

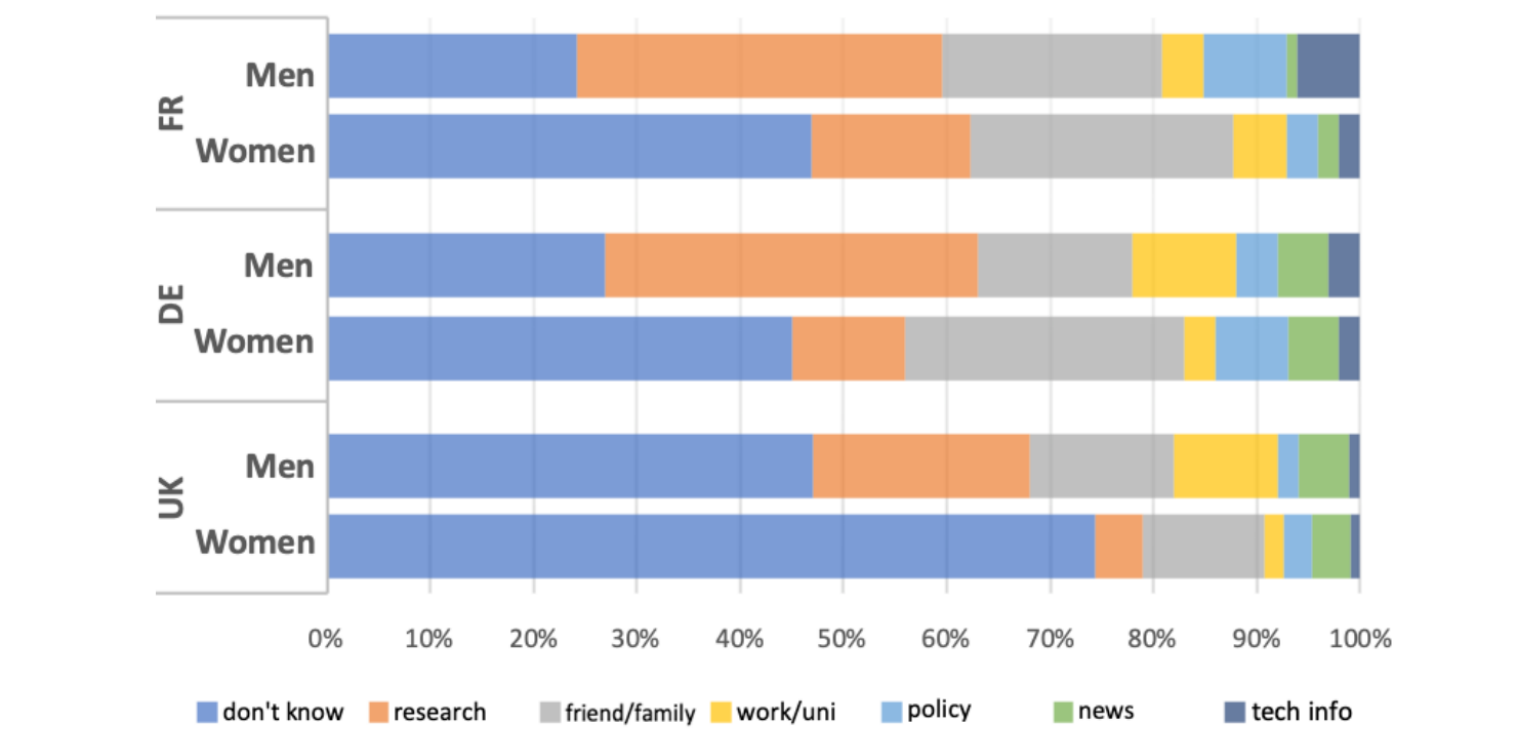
- RQ1: How do individuals learn about PETs for tracking protection?
- RQ2: What PETs do individuals use for TPT protection?
- 600 participants (Prolific Academic)

Country	N	Mean Age	Gender		
			#F	#M	#N
United Kingdom	209	35.78	109	100	0
Germany	202	29.21	100	100	2
France	203	27.29	98	99	6

*Note: for gender, F refers to female, M to male, and N to non-binary*

**Table 3.** Participant Characteristics

# Differences across Demographics



**Fig. 4.** % of participants learning about PETs for tracking protection via different methods.

Participants' use of  
 PETs by technology  
 type and how they  
 learn about them  
 (x-axis shows  
 number of  
 participants)

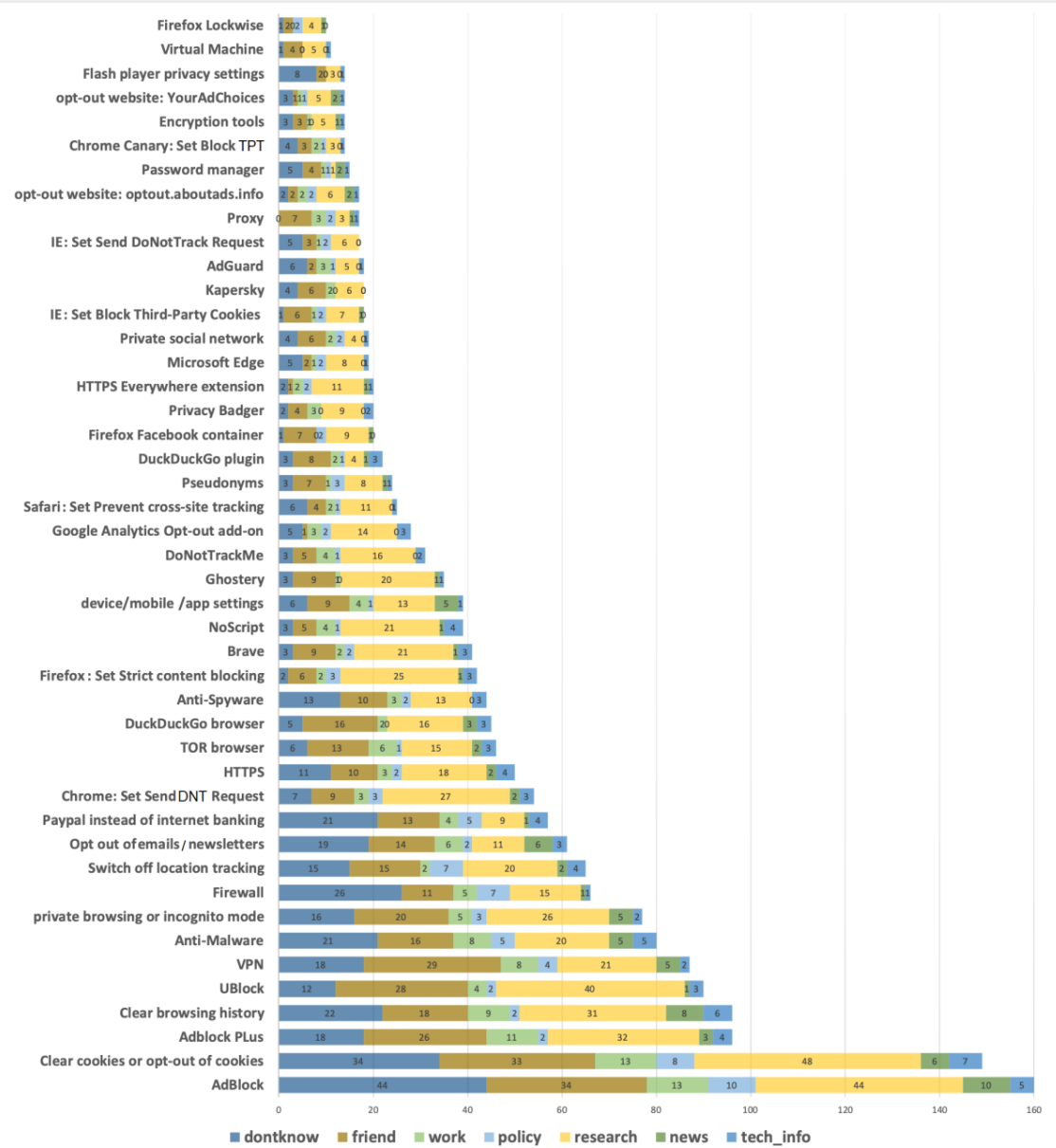


Fig. 6. Participants' use of PETs by technology type and how they learn about them (x-axis shows number of participants)

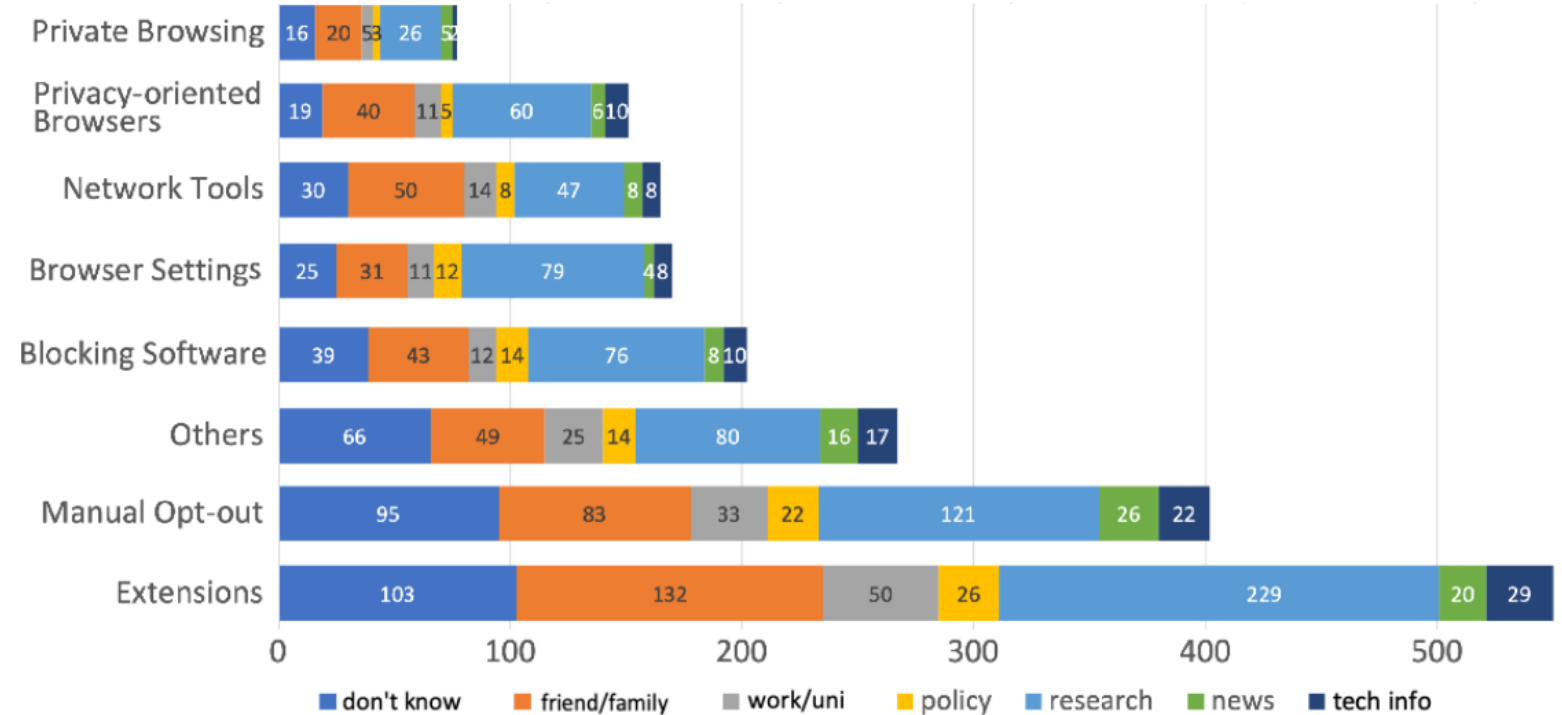
# PETs Employed by Participants

Type	Technology
Extensions	AdBlock, Adblock PLus, UBlock, NoScript, Ghostery, AdGuard DoNotTrackMe, Privacy Badger, Google Analytics Opt-out add-on, DuckDuckGo plugin, Firefox Facebook container, Firefox Lockwise, HTTPS Everywhere extension
Privacy-oriented Browsers	Brave, DuckDuckGo browser, Tor Browser and Microsoft Edge
Network Tools	Proxy, Virtual Machine, HTTPS, VPN
Browser Settings	Chrome Canary (builtin): Set Block third-party tracking, IE (builtin): Set Send DNT Request, IE (builtin): Set Block Third-Party Cookies, Safari (builtin): Set Prevent cross-site tracking, Firefox (builtin): Set Strict content blocking, Chrome (builtin): Set Send Do Not Track Request
Standalone Blocking Software	Anti-Malware, Kaspersky, Anti-Spyware, Firewall
Private Browsing	Private browsing or incognito mode option in modern browsers
Manual Opt-out	Clear cookies or opt-out of cookies, Clear browsing history, opt-out website: <a href="http://optout.aboutads.info">optout.aboutads.info</a> , opt-out website: YourAdChoices - <a href="http://Youronlinechoices.com">Youronlinechoices.com</a> , Switch off location tracking, Opt-out of receiving emails or newsletters
Others	Paypal instead of internet banking, device/mobile/app settings, Pseudonyms, Password manager, Private social network, Encryption tools, Flash player privacy settings

**Table 4.** The categorization of PETs technologies employed by our participants.



# PETs popularity among participants and ways of learning



**Fig. 5.** Number of participants using different categories of PETs & how they learn about them.

# Discussion

## Recommendations

- **Service providers** should aim for lawful, fair, and ethical practices.
- **PETs designers** make it clear what protection is and is not offered by particular PETs.
- **Users** can use privacy-oriented browsers.

## Online Privacy Regulations

- **Differences across demographics** should be identified by regulators.
- More effort is required to **enforce** the existing data protections laws.
- User privacy needs to be regulated on **other platforms** such as mobile and IoT.

# In Sum

- Opting-out is not as straightforward as accepting the default privacy settings.
- It becomes **more complicated** when users want to opt-out from previously accepted privacy settings (GDPR violation).
- We found **inconsistency** across regulations, websites, and user practices.
- Some of the methods practised by the users **do not prevent tracking** at all.
- We found an indication of a **'privacy gender gap'**.

**Part III:**

**Sensor Access on App vs Web**

# Risks of Mobile Ambient Sensors and User Awareness, Concerns, and Preferences

Maryam Mehrnezhad, Christodoula Makarouna, Danté Gray

Paper at The European Symposium on Usable Security

2022

# Introduction

- More than 30 sensors on off-the-shelf mobile phones
- Different categories: biometric, communicational, motion, and ambient sensors.
- Ambient sensors are less studied for their security and privacy risks
- Access to such sensors across platforms: Apps, Web, IoT

Table 1. List of ambient sensors found in off-the-shelf mobile devices

Sensor	Unit	Data Description	Sensor	Unit	Data Description
Light	lx	Illuminance	Magnetic Field	$\mu T$	Geomagnetic field strength
Pressure	hPa/mbar	Ambient air pressure	Hall Sensor	$\mu T$	Magnetic field strength
Humidity	%	Ambient relative humidity	Air Sensor	NA	Chemical pollutants level
Ambient Temp	$^{\circ}C$	Ambient air temperature	Proximity	cm	Distance from object
Device Temp	$^{\circ}C$	Device temperature	Laser	cm	Depth & distance from object
Gravity	$m/s^2$	Force of gravity			

# Actual Risks

- Mobile
- IoT Systems

- **Location Tracking**
  - instead of using GPS directly
- **Eavesdropping**
  - e.g. recovering speech
- **Keystroke Monitoring**
  - PINs, passwords, and lock patterns
- **User (activities) Identification**
  - individual's patterns and activities
- **Device Fingerprinting**
  - profiling users

# User Studies

- Mobile users are **not** generally **familiar** with most mobile sensors.
- There is a **disparity** between the actual and perceived risk levels of sensors.
- **Teaching** does not improve the user risk perception, User's prior **knowledge** has a stronger impact.
- No studies on user perception and preferences for ambient sensors via **app vs web**.
- No studies on users perspective on the use of **AI/ML** for managing sensors on their behalf.



# Online Survey with 197 Participants

## Sections:

- 1. Mobile ambient sensors
- 2-3. Technology demographics and general security & privacy
- 4. Protection preferences
- Risks
- 6-7. Revisited questions and Smart system
- 8. Demographics and Consent

## Methodology:

- Mixed method of quantitative and qualitative analysis
- Thematic analysis

## Participants:

- UK/EU participants recruited via email lists, messaging apps, social media.
- 50% female, 49.5% male, 0.5% other, 18-63 yrs old, various jobs

RESULTS



# Not Familiar and Not Concerned

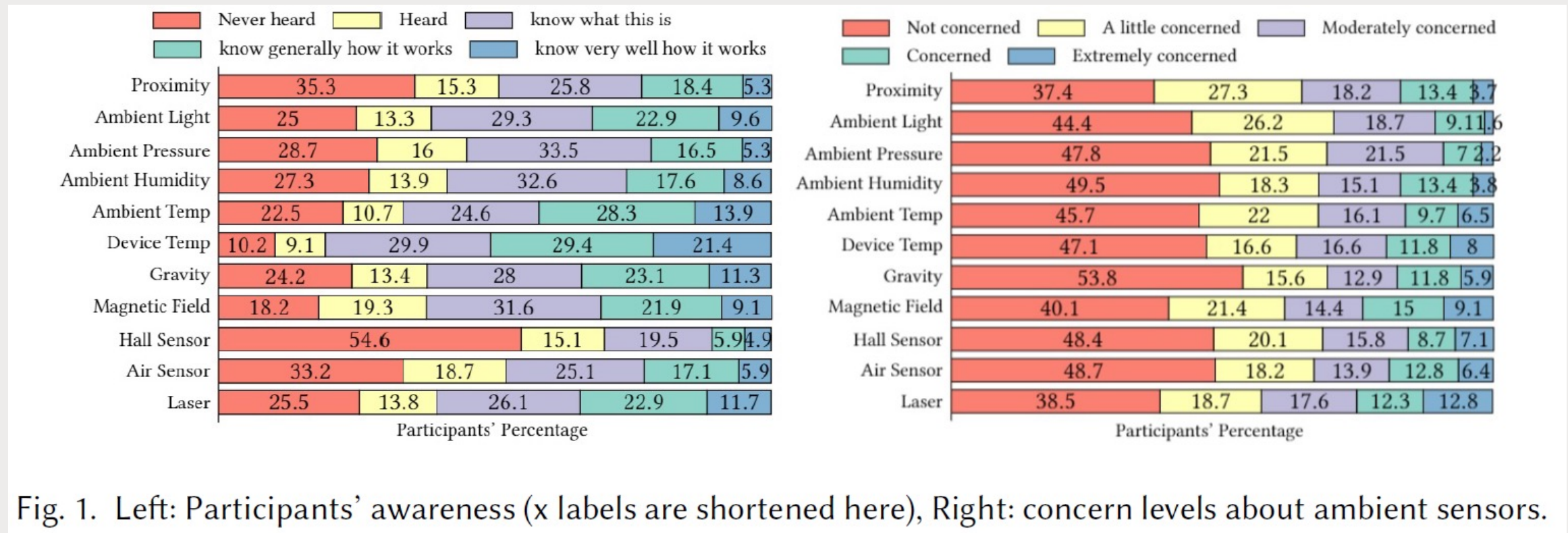


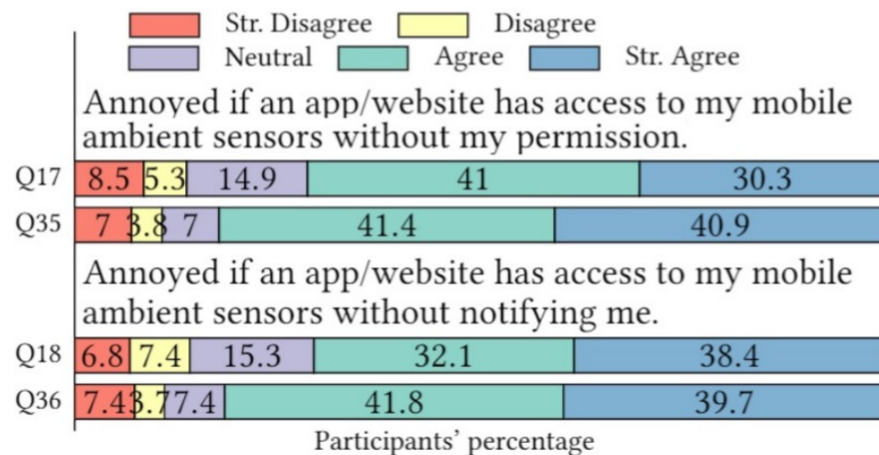
Fig. 1. Left: Participants' awareness (x labels are shortened here), Right: concern levels about ambient sensors.

# Annoyed if app/website has access to ambient sensors without permission

## Would like some form of control (install time, first open, each use, regularly)

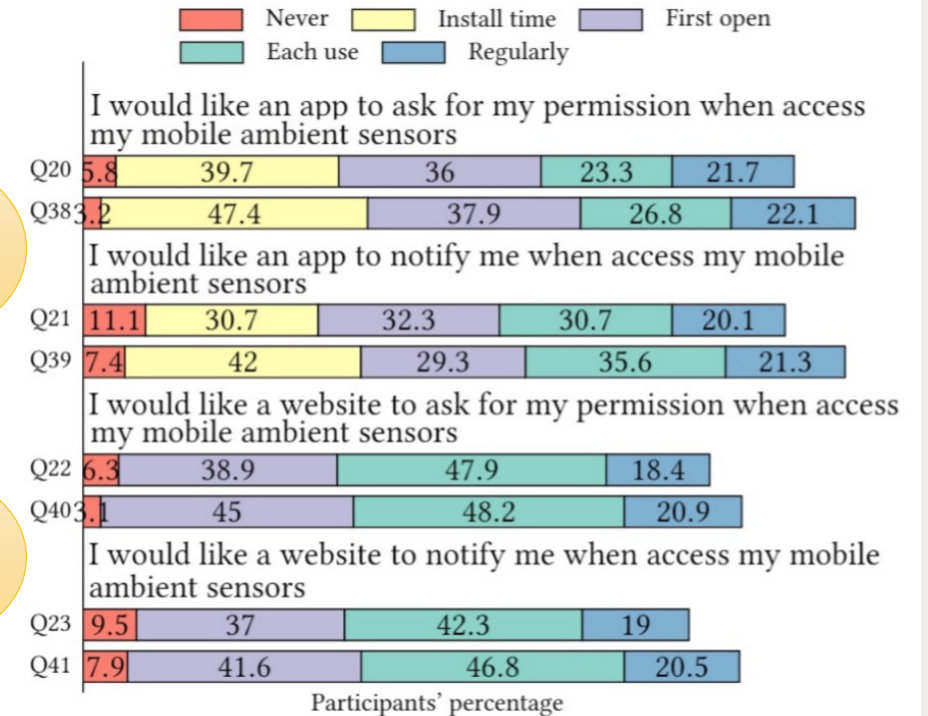
Fig. 2. Left: Participant annoyance about app/website access to ambient sensors when first asked (Qs17-18) and after being introduced to sensor risks (Qs36-37).

Right: Participant views on permission models for mobile ambient sensors when first asked (Qs20-23) and after being introduced to sensor risks (Qs38-41).



App

Web



# Specifically worried if ambient sensors reveal their Location

## ■ User comments:

- *Lack of consent*
- *Violation of privacy*
- *Malicious usage*

"Its an invasion of my privacy and a risk to the safety of my child and myself "

'exploited', 'insecure', 'monitored', 'spied on', 'creepy', 'tracked', etc.

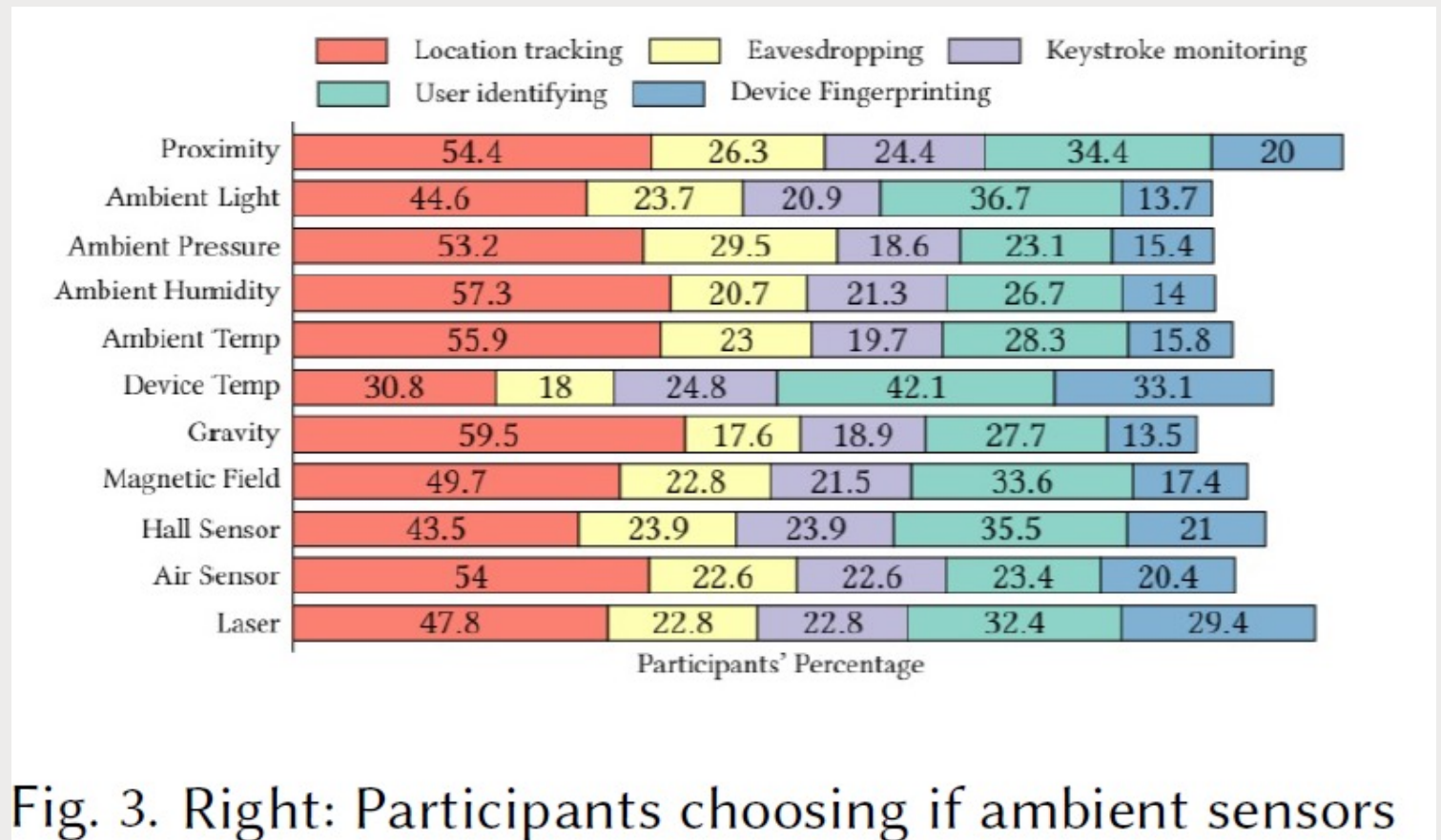


Fig. 3. Right: Participants choosing if ambient sensors

# Protective actions are consistent across platforms (App and Website)

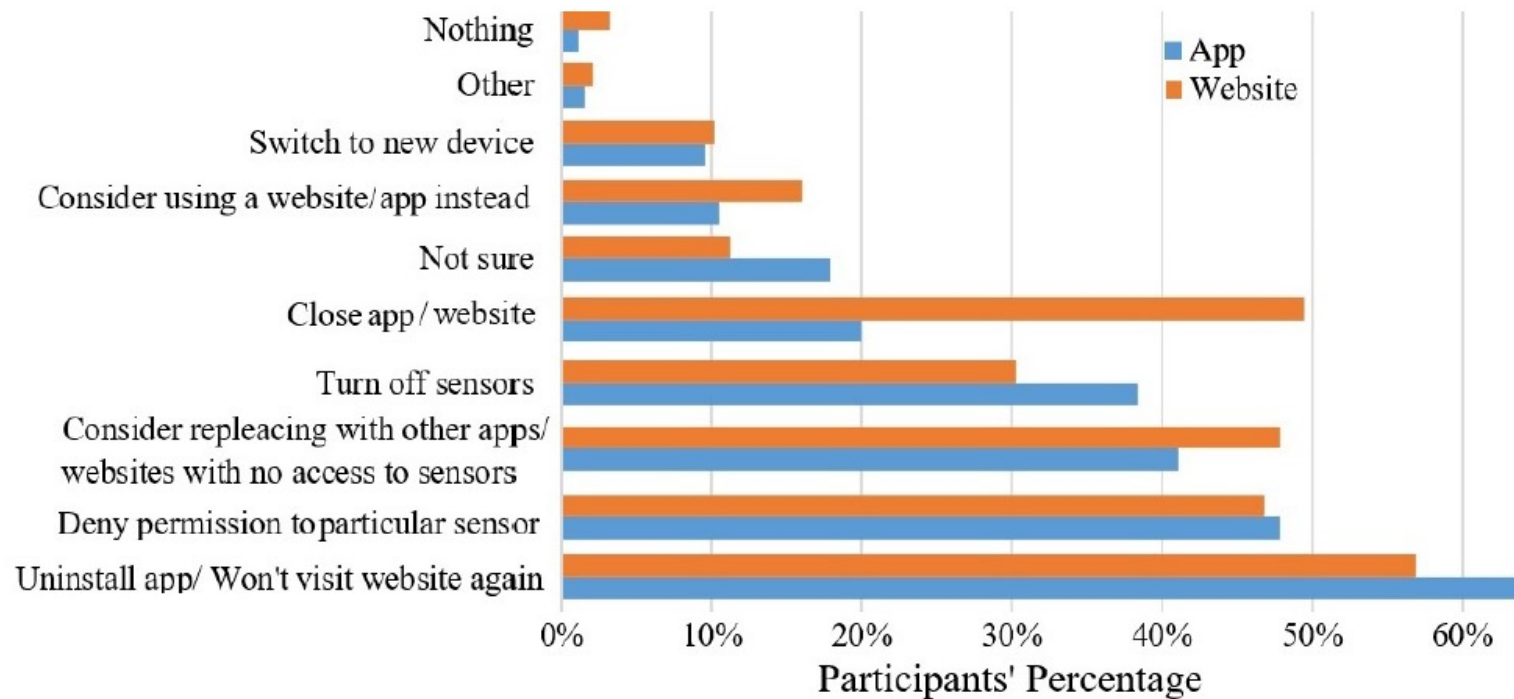


Fig. 4. Potential actions taken by participants in case of sensor leakage in Apps and Websites.

# Smart Sensor Management System

Table 3. Extracted themes form user comments on features of a smart sensor management system.

<b>General Features</b>	no. (%)	<b>Preferred Risk Notification</b>	no. (%)	<b>Annoying Risk Notification</b>	no. (%)
Control	30 (15%)	Distinguishable	36 (19%)	Repetitive	52 (26%)
Security & Privacy	20 (10%)	Communication Channel	10 (5%)	Poor User Interface	25 (13%)
Usability	25 (12%)	Including Details	24 (11%)	No Control/Customisation	14 (7%)
		Simple	18 (8%)	False Alert	13 (7%)
		Requiring User Action	14 (7%)		



## Control



- “Check and confirm that ambient sensor are used only with **my permission**, and if not to notify me immediately.”
- “**Giving you control** whenever you want to check the use of your device and sensors”,
- “specify why an app needs access to these and **ask for approval**”.

## Usability



- “It would be easier to manage permissions; especially, with a **feature for grouping similar apps** to manage their access permissions as a group rather than once for each app”.
- “It should allow me to **easily** revoke sensor access and re-enable it when an app absolutely needs it.”

## Security & Privacy



- “It [smart system] should respond to news about **leaks** to apps and automatically restrict the app or containerized it with fake sensor data.”
- “[such a system would] **protect privacy** and keep users safe while running in background of device.”



# Results across Demographics

## ■ Gender:

- Male participants expressed more knowledge about sensors/risks than female participants.
- Female participants expressed more concerns in relation to their privacy and security being at risk via sensors.

## ■ Age:

- Younger the participants prefer to involve in permission controlling less often

## ■ Operating System:

- No significant differences

# Discussion

- **Real-world practices:** no permission, “We just have to learn to live with the idea that everything we do is trackable and is being recorded.”
- **Regulations:** ongoing problem, “People should be informed and be aware of the risks. Legislation should protect the end user by such privacy breaches.”
- **User-centric solutions:** ML/AI: “A smart system which is designed in a centralised way to restrict access to sensor data would be very good for people less aware of what might be collected about them and protect them from security risks/attacks.”

# Summary

Risks of Mobile Ambient Sensors and  
User Awareness, Concerns, and Preferences

[Maryam.Mehrnezhad@rhul.ac.uk](mailto:Maryam.Mehrnezhad@rhul.ac.uk)

Twitter: maryammjd

- The majority of our participants are **not/little concerned** about ambient sensors and risks.
- The majority would be (very) **upset** if ambient sensors contribute to potential risks
- Participants' views on **permission models** and **protection actions** were **consistent** across platforms (app and website).
- Majority preferred a **smart management system** to handle sensors on their behalf