PERC_LAB
Home of Privacy Engineering – Regulatory Compliance Research

1865 THE UNIVERSITY OF MAINE

Evaluating Privacy Perceptions, Experience, and Behavior of Software Development Teams

Maxwell Prybylo, Sara Haghighi, Sepideh Ghanavati, Sai Teja Peddinti
University of Maine Google Inc.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024
August 11–13, 2024

NSF

Introduction

- **Privacy violations** are increasing all around the world.
- Adopting **new privacy regulations** in many countries.
- Increasing pressure on developers when implementing privacy solutions.

Developers' Privacy Challenges

- ❑ Most small development teams often **lack the privacy expertise and legal resources** needed to make informed decisions about privacy.

The lack of these resources hinders the development of clear, precise, and uniform **privacy policies.**

Key Research Questions

RQ1 Are there any differences in privacy perceptions among various roles, locations, and other demographics?

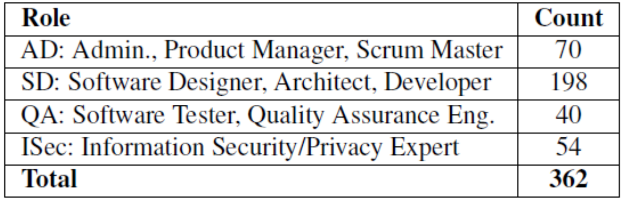
RQ2 Does access to privacy experts (e.g., a Chief Privacy Officer – CPO) impact privacy perceptions and practices?

RQ3 How do privacy practices and experiences vary according to SDLC roles, locations, and other demographics?

RQ4 What is the degree of familiarity of different roles regarding privacy concepts, approaches, tools, and regulations?

Study Design

- **Mixed-method** survey study using Qualtrics on the Prolific platform.



Role	Count
AD: Admin., Product Manager, Scrum Master	70
SD: Software Designer, Architect, Developer	198
QA: Software Tester, Quality Assurance Eng.	40
ISec: Information Security/Privacy Expert	54
Total	**362**

Participants

- 362 from 23 countries

Regions

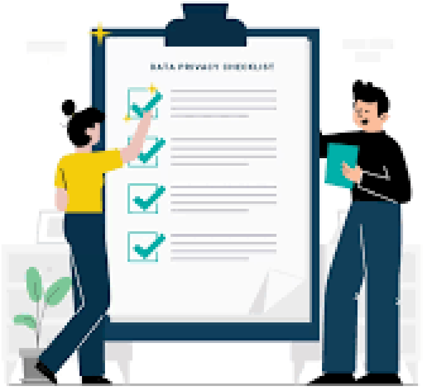
- US, EU+UK, South Africa, Mexico, Canada, South America

Roles

- Product managers, developers, QA, information security/privacy experts, etc.

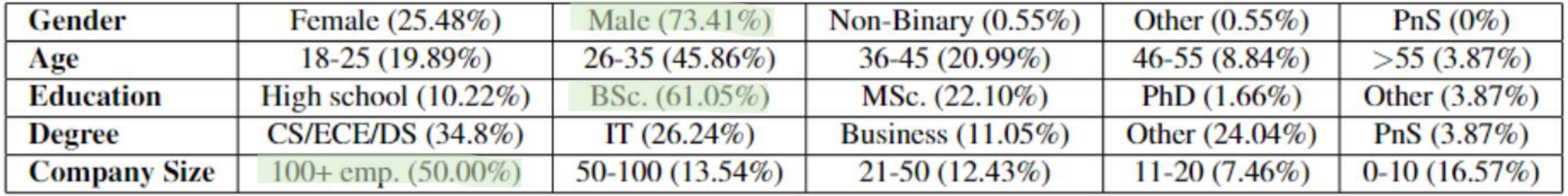
Survey Sections

- Demographics, general privacy questions, role-specific questions



Demographic Information

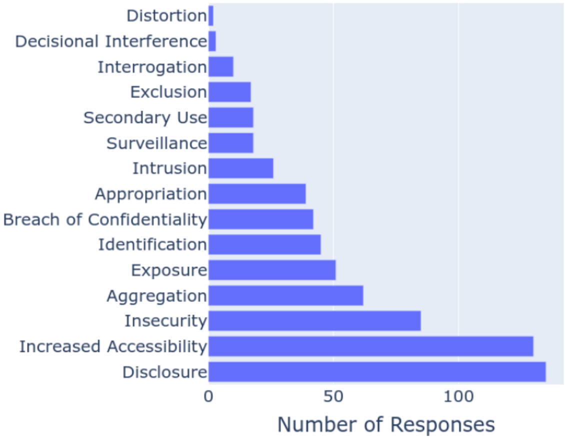
- Most participants identify as **male**, are **below the age of 45**, and have completed their **BSc**., With ~61% in Computer Science (CS), Information Technology (IT), Data Science (DS), and Electrical & Computer Engineering (ECE) majors.
- Half of them work in a company with **more than 100** employees.



Gender	Female (25.48%)	Male (73.41%)	Non-Binary (0.55%)	Other (0.55%)	PnS (0%)
Age	18-25 (19.89%)	26-35 (45.86%)	36-45 (20.99%)	46-55 (8.84%)	>55 (3.87%)
Education	High school (10.22%)	BSc. (61.05%)	MSc. (22.10%)	PhD (1.66%)	Other (3.87%)
Degree	CS/ECE/DS (34.8%)	IT (26.24%)	Business (11.05%)	Other (24.04%)	PnS (3.87%)
Company Size	100+ emp. (50.00%)	50-100 (13.54%)	21-50 (12.43%)	11-20 (7.46%)	0-10 (16.57%)

Findings – Privacy Perceptions

- **Definitions of Privacy**
  - ✓ The variety of privacy definitions shows the complexity of privacy perceptions.



- **Confidence in Security and Privacy Measures**
  - ✓ ISec members were **the most** confident, while QA members were **the least** confident.
  - ✓ **No correlation** was found between confidence and demographic factors.

Findings – Privacy Perceptions

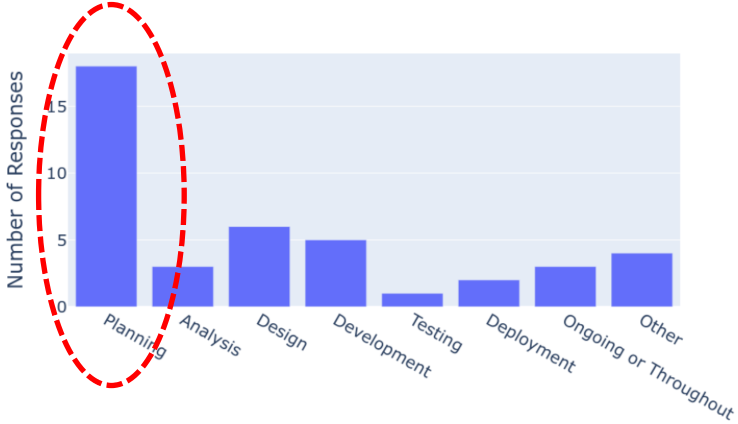
- **Presence of a Chief Privacy Officer (CPO)**
  - ✓ **<u>Larger companies</u>** are more likely to have a CPO.
  - ✓ Significant **correlation** between the presence of a CPO and increased confidence in privacy and security measures.

    However,

    it has **limited effectiveness** in enhancing privacy practices and reducing breaches.

Findings - Privacy Practices

- **Privacy Impact Assessments (PIAs):**



✓ Most team members are **unfamiliar** with or unaware of PIA creation.

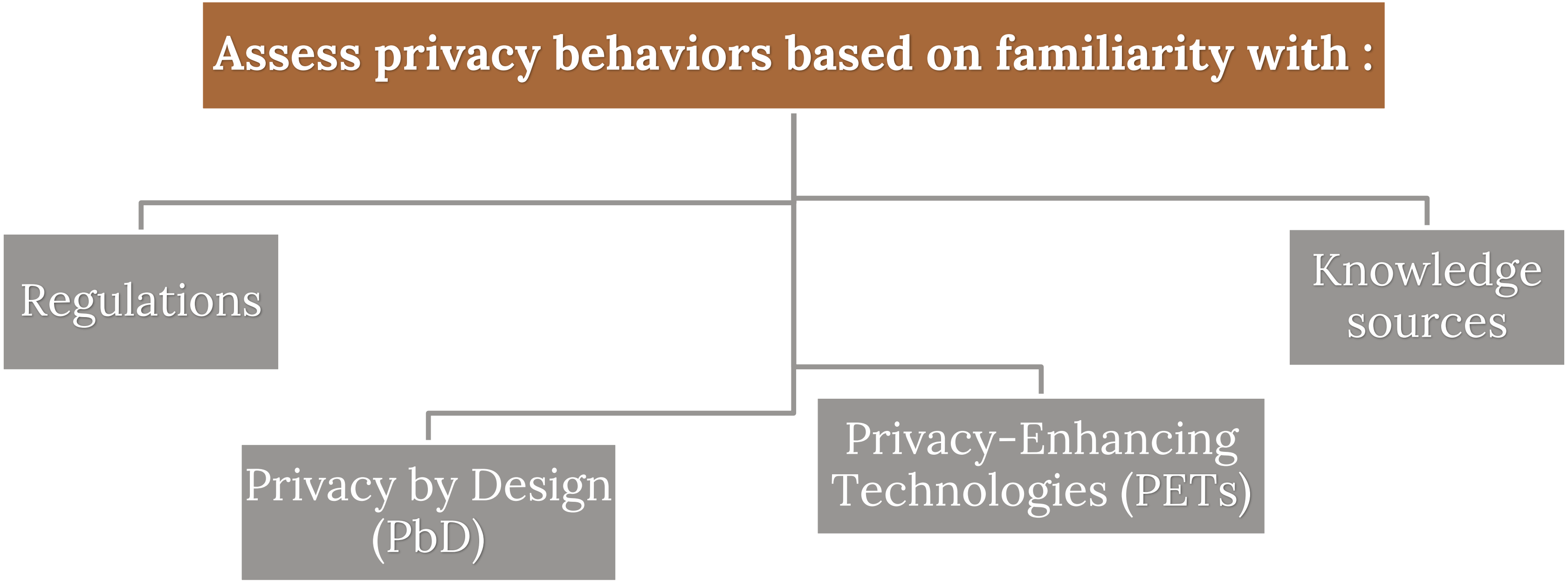
✓ **Significant correlation** between PIA creation and company size

Findings - Privacy Practices

- **Creation of Privacy Policies:**

1. Primarily handled by legal experts (64%)
2. Use of templates (45.5%) and privacy policy generators (36.4%)
3. Compliance with regulations, and ensuring completeness and correctness are among the most common challenges

Findings - Privacy Awareness and Behaviors



Assess privacy behaviors based on familiarity with :

Regulations

Privacy by Design (PbD)

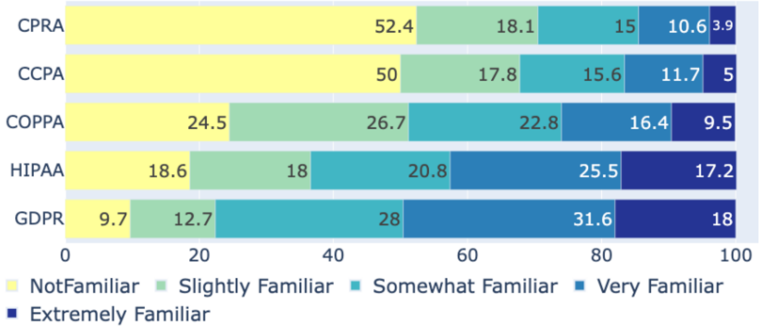
Privacy-Enhancing Technologies (PETs)

Knowledge sources

Findings - Privacy Awareness and Behaviors

Assess privacy behaviors based on familiarity with:

Regulations

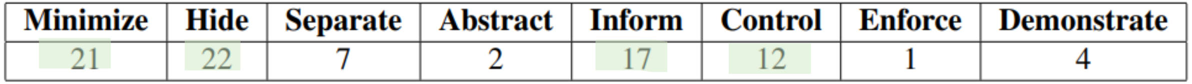


- ✓ **GDPR** is the most familiar regulation.
- ✓ ISec teams are **more familiar** with regulations.
- ✓ QA teams are the **least familiar**.

Findings - Privacy Awareness and Behaviors

Assess privacy behaviors based on familiarity with :

PbD



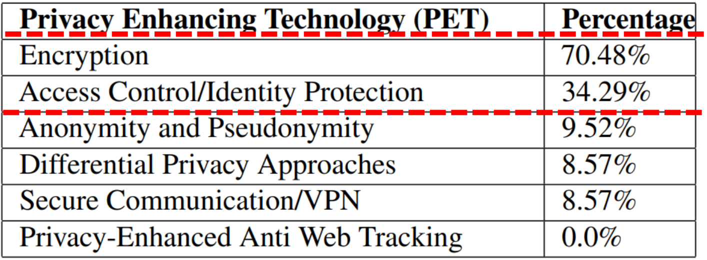
Minimize	Hide	Separate	Abstract	Inform	Control	Enforce	Demonstrate
21	22	7	2	17	12	1	4

- ✓ PbD approaches are **not** yet commonly used.
- ✓ Limited **awareness** (46%) and **usage** (57.1%) among developers.
- ✓ Need for better integration of PbD in development processes.
- ✓ Gaps in **usability and readiness** of PbD for day-to-day tasks.

Findings - Privacy Awareness and Behaviors

Assess privacy behaviors based on familiarity with :

PETs



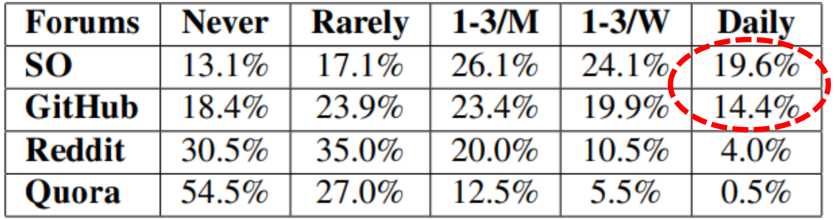
Privacy Enhancing Technology (PET)	Percentage
Encryption	70.48%
Access Control/Identity Protection	34.29%
Anonymity and Pseudonymity	9.52%
Differential Privacy Approaches	8.57%
Secure Communication/VPN	8.57%
Privacy-Enhanced Anti Web Tracking	0.0%

- ✓ PETs are more commonly used than PbDs.
- ✓ More than 40% of developers do **not** use them.
- ✓ Developers use more **security-oriented** PETs rather than **privacy-oriented** ones.

Findings - Privacy Awareness and Behaviors

Assess privacy behaviors based on familiarity with :

Knowledge sources

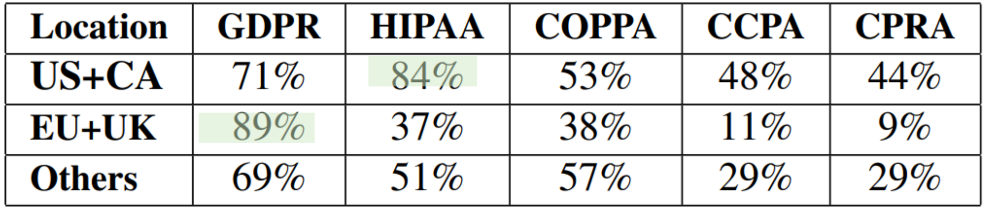


Forums	Never	Rarely	1-3/M	1-3/W	Daily
SO	13.1%	17.1%	26.1%	24.1%	19.6%
GitHub	18.4%	23.9%	23.4%	19.9%	14.4%
Reddit	30.5%	35.0%	20.0%	10.5%	4.0%
Quora	54.5%	27.0%	12.5%	5.5%	0.5%

- ✓ More than 50% of participants use either **Stack Overflow** or **GitHub** to seek privacy-related information.

Location Analysis

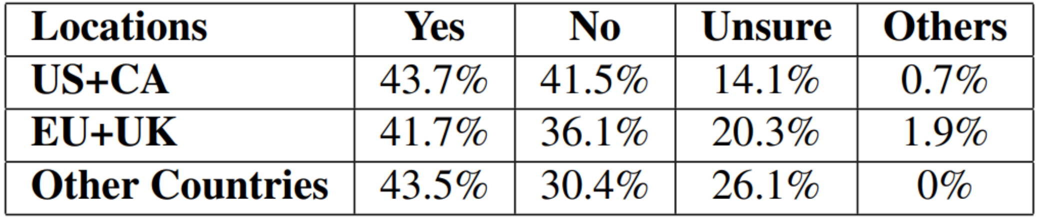
- **Regulation Familiarity**:
  - ✓ **Higher familiarity** with **GDPR** (EU+UK) and **HIPAA** (US+CA).
  - ✓ **COPPA**, **CCPA**, and **CPRA** **less known** outside US+CA.



Location	GDPR	HIPAA	COPPA	CCPA	CPRA
US+CA	71%	84%	53%	48%	44%
EU+UK	89%	37%	38%	11%	9%
Others	69%	51%	57%	29%	29%

Location Analysis

- **Impact of Location and Challenges**:
  - ✓ Need consistent privacy practices across regions.
  - ✓ Correlation between company size and presence of a CPO.
  - ✓ No significant differences in privacy practices between regions.



Locations	Yes	No	Unsure	Others
US+CA	43.7%	41.5%	14.1%	0.7%
EU+UK	41.7%	36.1%	20.3%	1.9%
Other Countries	43.5%	30.4%	26.1%	0%

Distribution of Location-based CPO Presence

Discussion and Key Takeaways

- **Research Directions:**
  - ✓ **Translate** privacy-related questions into accurate code snippets.
  - ✓ Focus on **automated legal/privacy requirement extraction** and user stories for agile development.
  - ✓ **Automated** monitoring and compliance nudges are needed.
- **Educational Takeaway:**
  - ✓ Courses should cover **advanced privacy topics** and distinguish from security.
  - ✓ Foster life-long learning of **dynamic privacy concepts**.
  - ✓ **Online tools** for privacy-preserving solutions are crucial.

Conclusion and Future Directions

- **Summary**:

Examined privacy perceptions, practices, and behaviors of SDLC team members during software development.

- **Future Work**:
  - ✓ Conduct a comparative analysis within US states.
  - ✓ Evaluate whether developers over-claim their expertise.
  - ✓ Investigate how privacy is taught at educational institutions, both in computer science and law schools.

Thanks!

Any questions?

Maxwell Prybylo
University of Maine
maxwell.prybylo@maine.edu

Sara Haghighi
University of Maine
sara.haghighi@maine.edu

Sai Teja Peddinti
Google
psaiteja@google.com

Sepideh Ghanavati
University of Maine
sepideh.ghanavati@maine.edu