

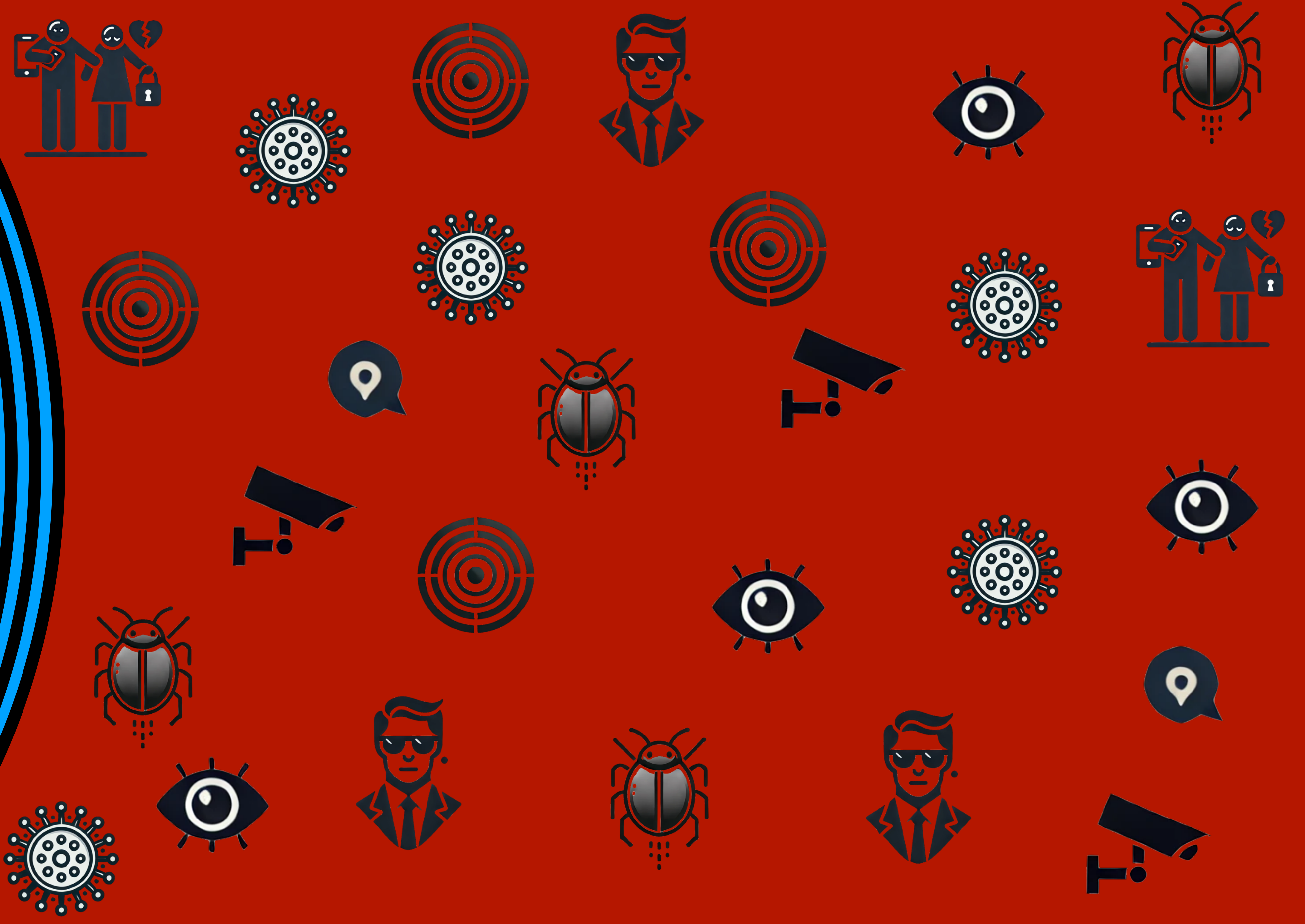
A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

Omer Akgul^M • Sai Teja Peddinti^G • Nina Taft^G • Michelle L. Mazurek^M
Hamza Harkous^G • Animesh Srivastava^G • Benoit Seguin^G



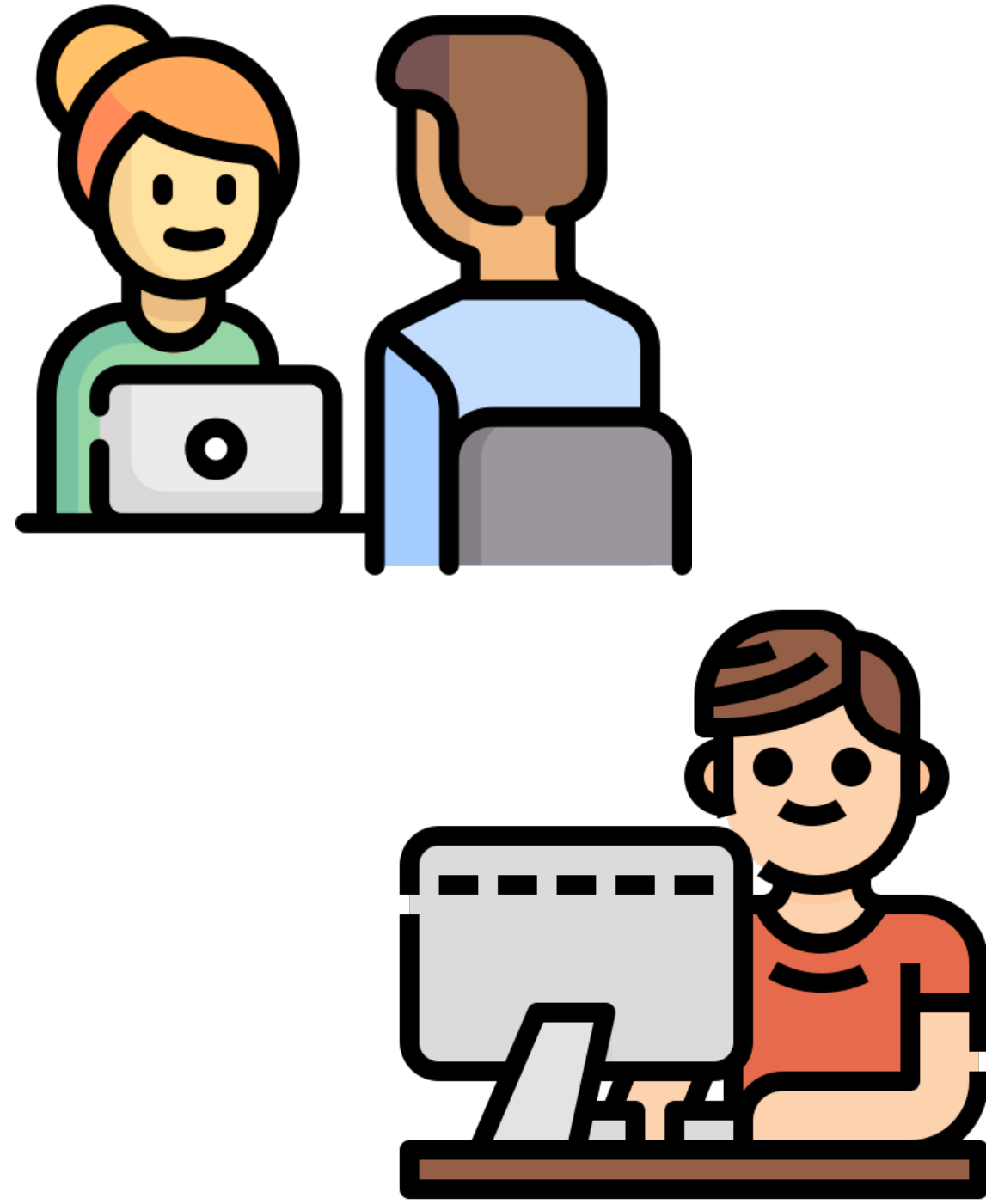
UNIVERSITY OF
MARYLAND



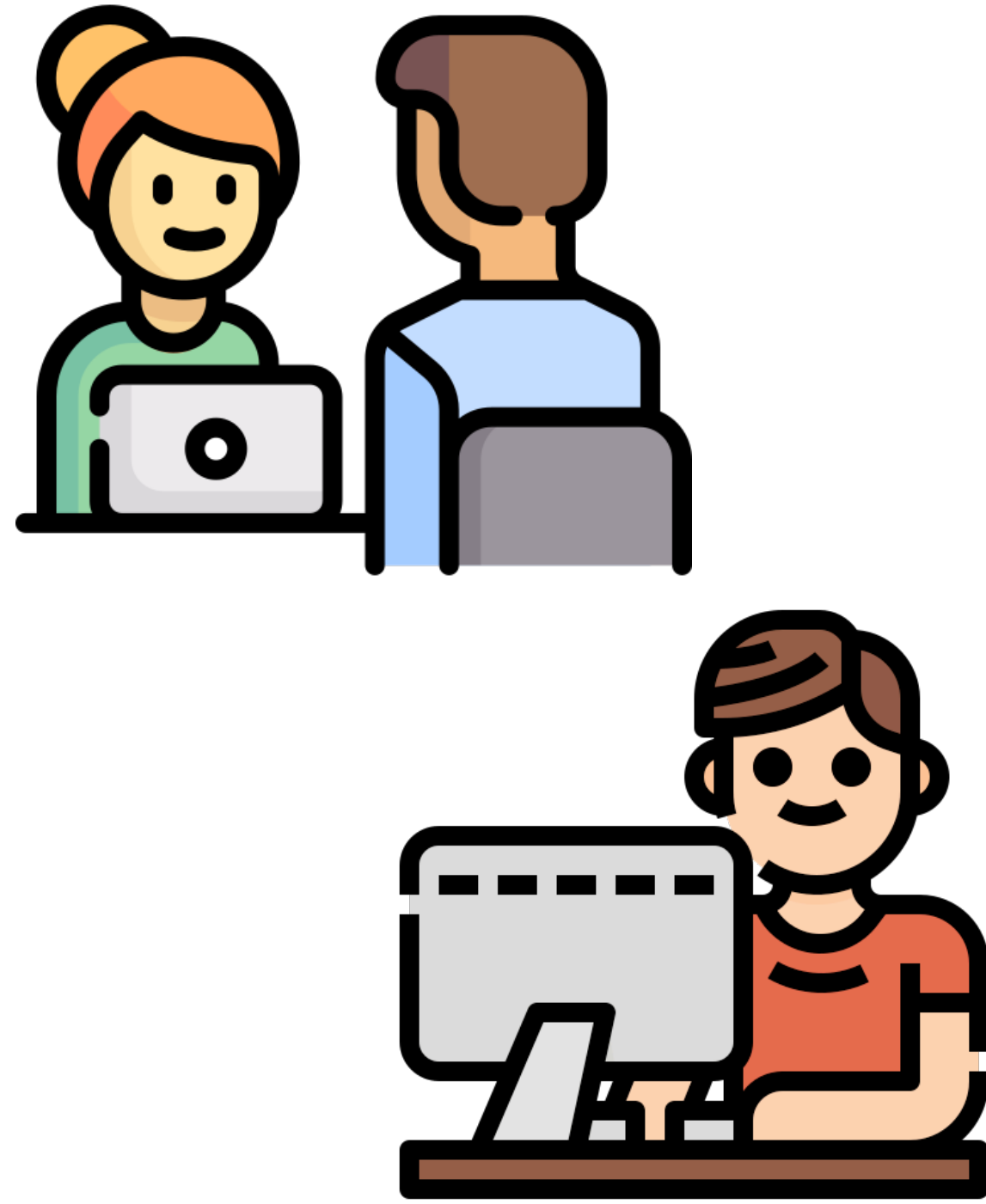


Measuring privacy sentiment is hard

Measuring privacy sentiment is hard



Measuring privacy sentiment is hard



A/B

Privacy-relevant feedback

Privacy-relevant feedback

- User-feedback is plentiful



Privacy-relevant feedback

- User-feedback is plentiful
- Multiple sources



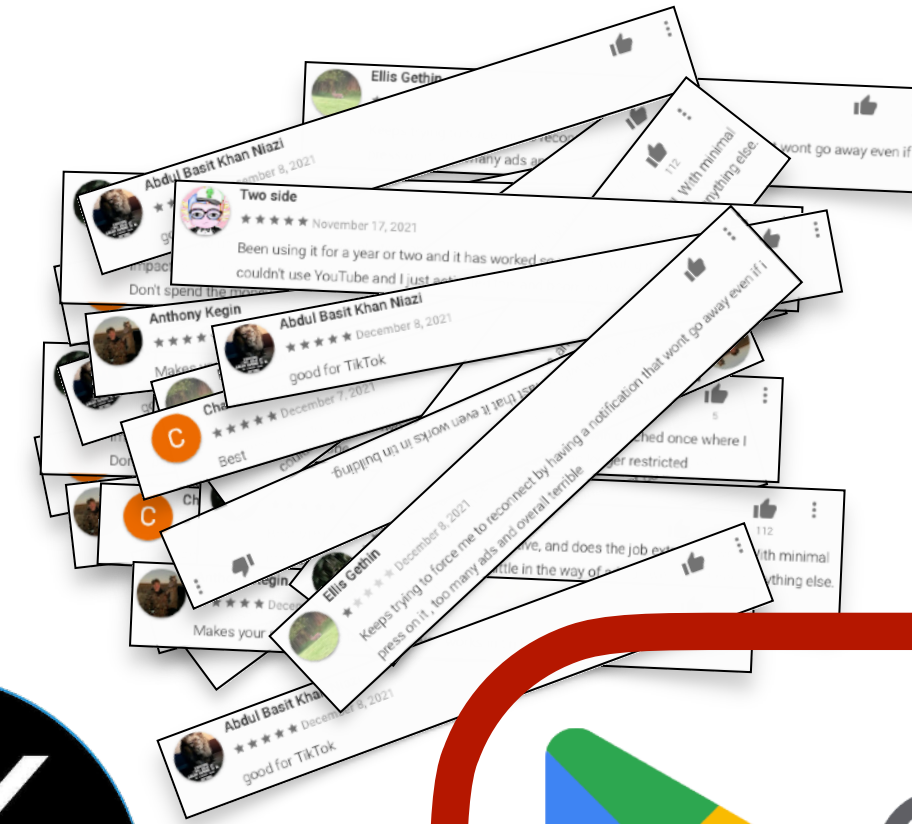
Privacy-relevant feedback

- User-feedback is plentiful
- Multiple sources



Privacy-relevant feedback

- User-feedback is plentiful
- Multiple sources



Privacy-relevant feedback

- User-feedback is plentiful
- Multiple sources
- Our focus: user feedback that includes discussion of privacy.



Privacy-relevant feedback

- User-feedback is plentiful
- Multiple sources
- Our focus: user feedback that includes discussion of privacy.
- Commonly used in prior work



Privacy-relevant feedback

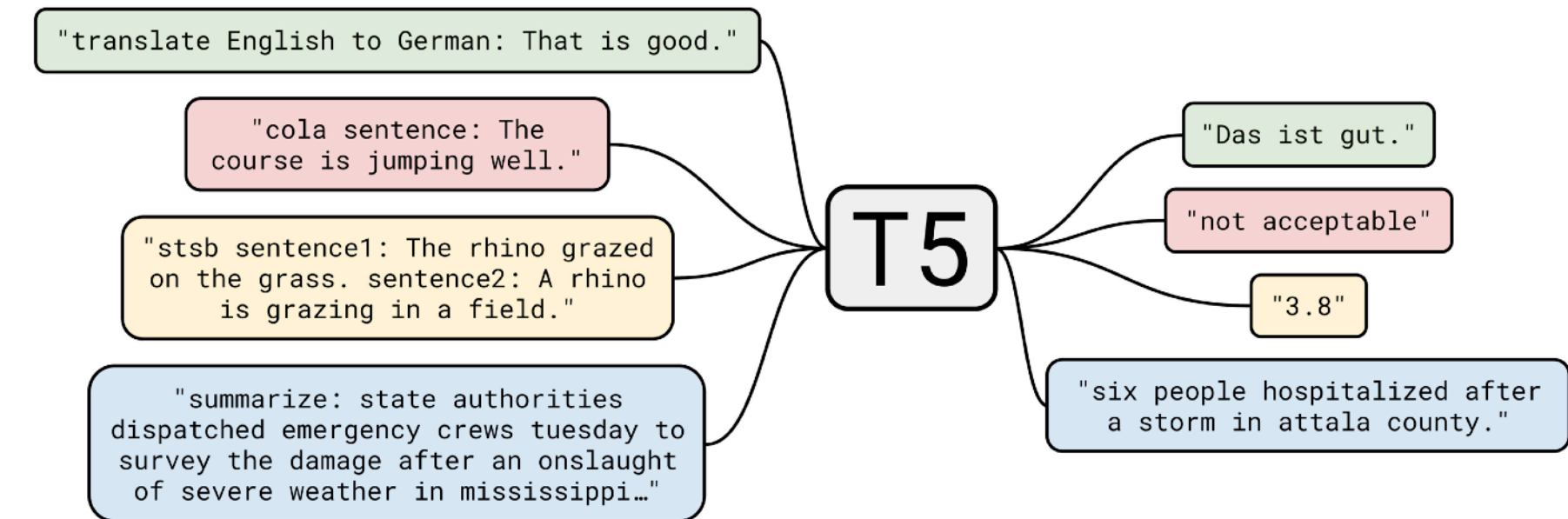
- User-feedback is plentiful
- Multiple sources
- Our focus: user feedback that includes discussion of privacy.
- Commonly used in prior work
- We saw inefficiencies



How to make privacy reviews digestible?

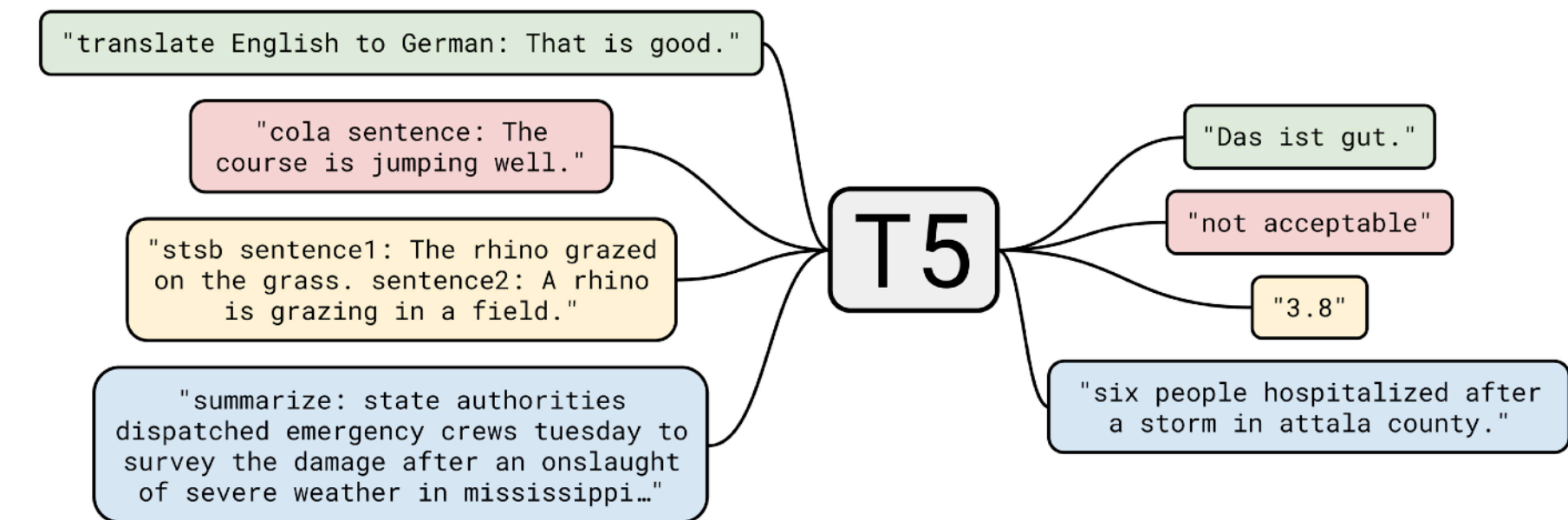
How to make privacy reviews digestible?

- Why not process this data with language models?



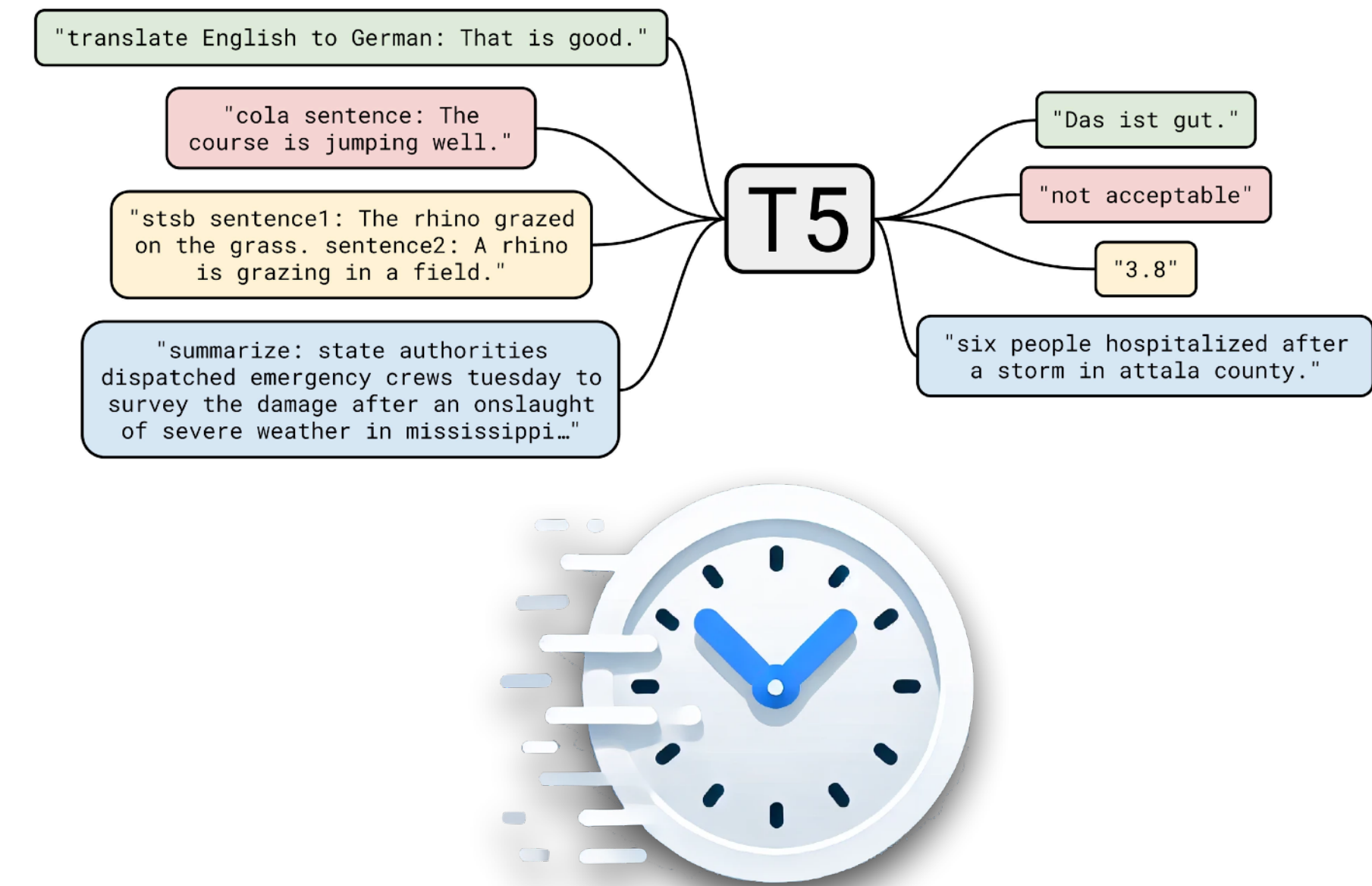
How to make privacy reviews digestible?

- Why not process this data with language models?
- Allows for processing of lots of data, generalizability.



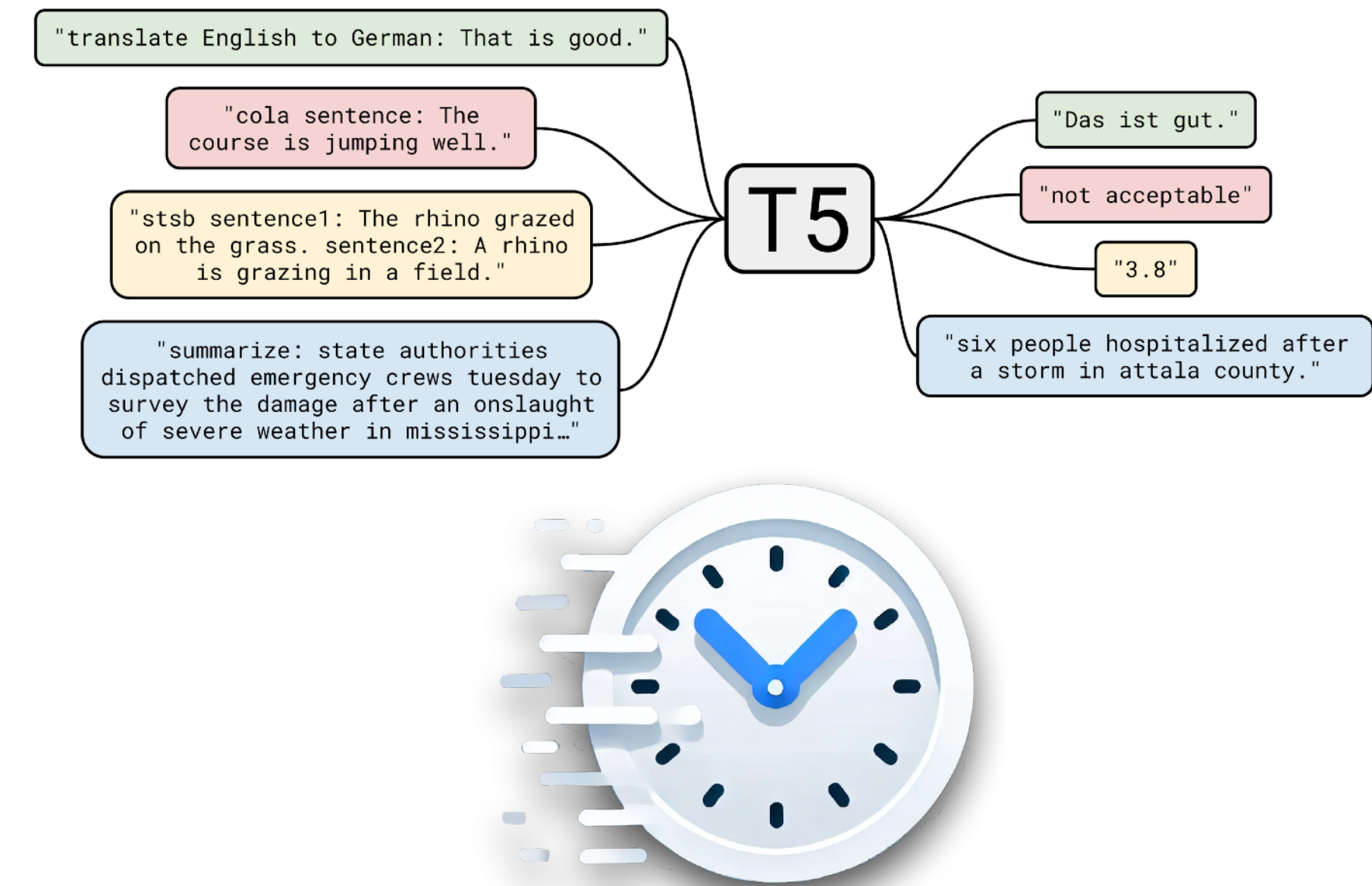
How to make privacy reviews digestible?

- Why not process this data with language models?
- Allows for processing of lots of data, generalizability.
- Quick and high-level insights



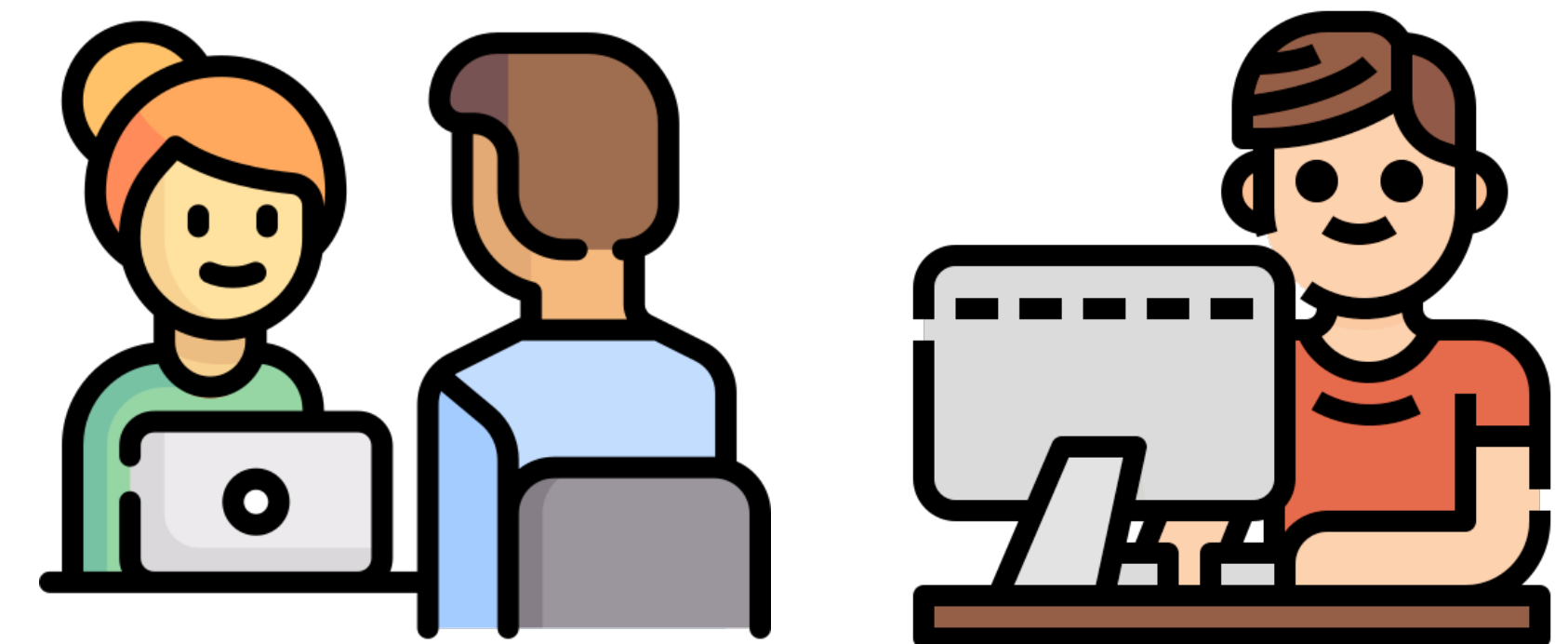
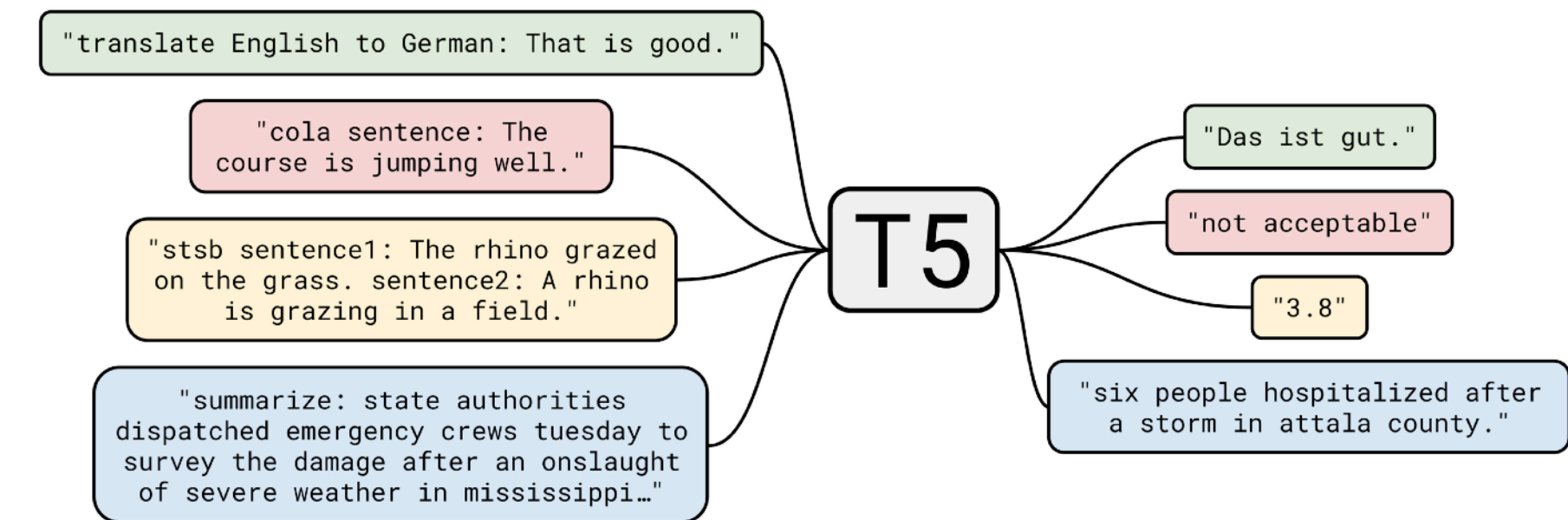
How to make privacy reviews digestible?

- Why not process this data with language models?
- Allows for processing of lots of data, generalizability.
- Quick and high-level insights
- Add context to prior work, find gaps in research.



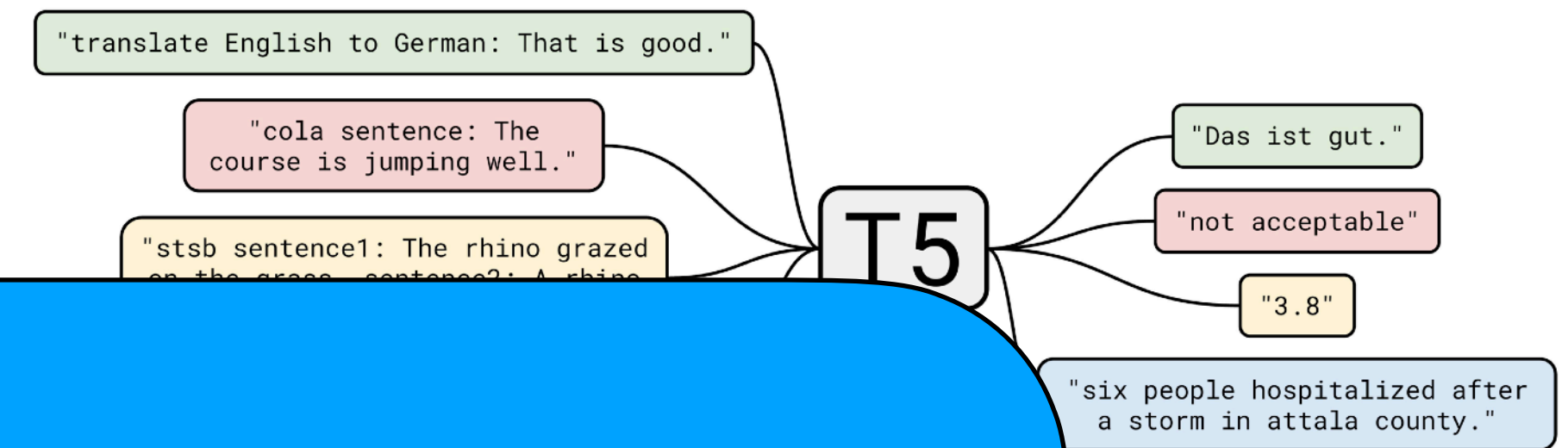
How to make privacy reviews digestible?

- Why not process this data with language models?
- Allows for processing of lots of data, generalizability.
- Quick and high-level insights
- Add context to prior work, find gaps in research.
- Complementary to existing methods.

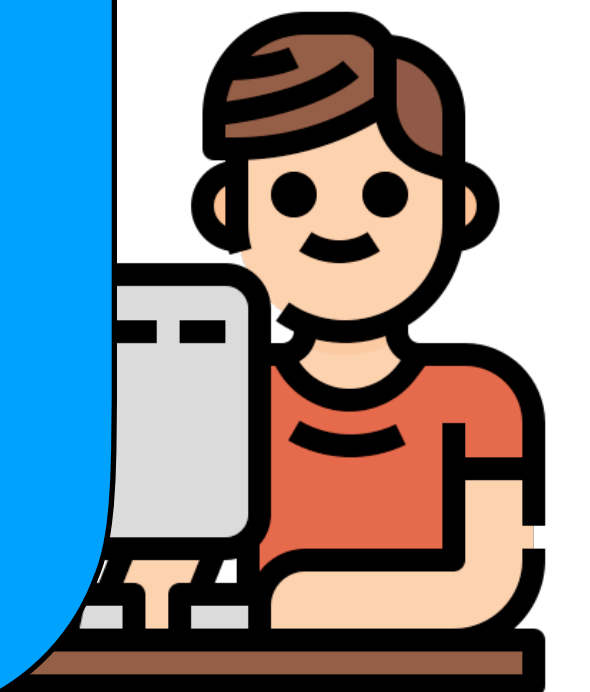


How to make privacy reviews digestible?

- Why not process this data with language models?

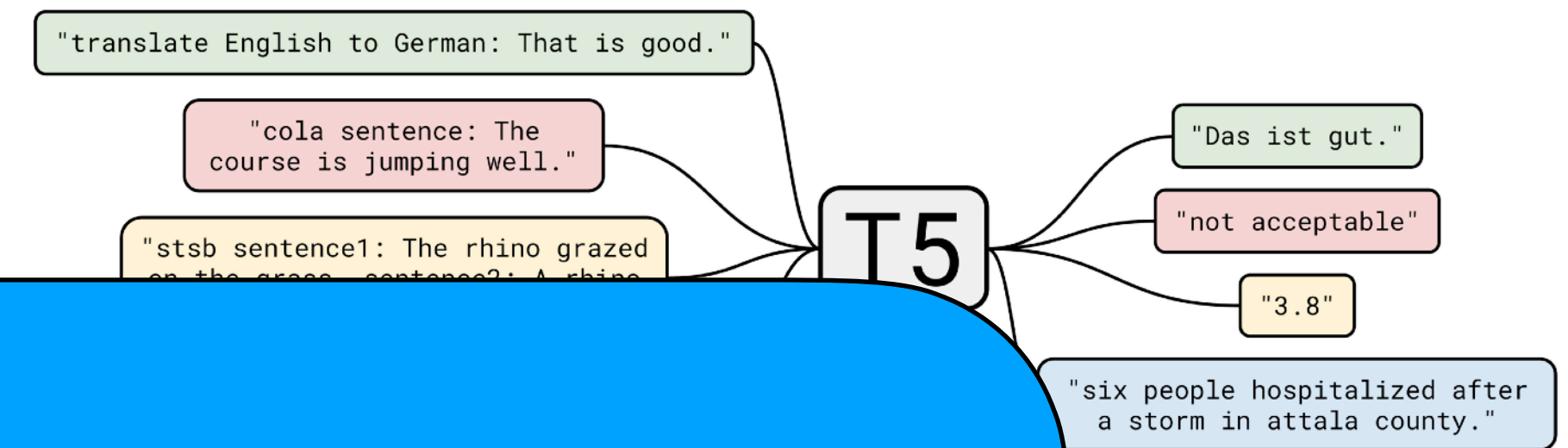


- Allow gener...
- Quick...
- Add resear...
- Comp...



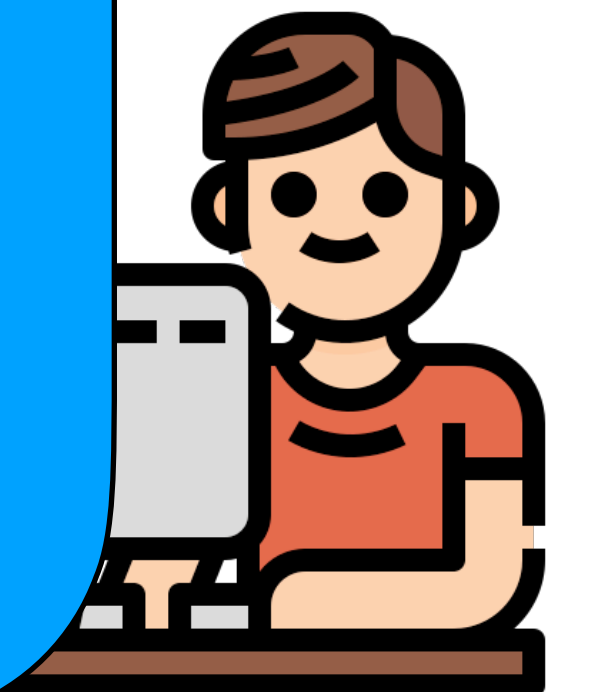
How to make privacy reviews digestible?

- Why not process this data with language models?



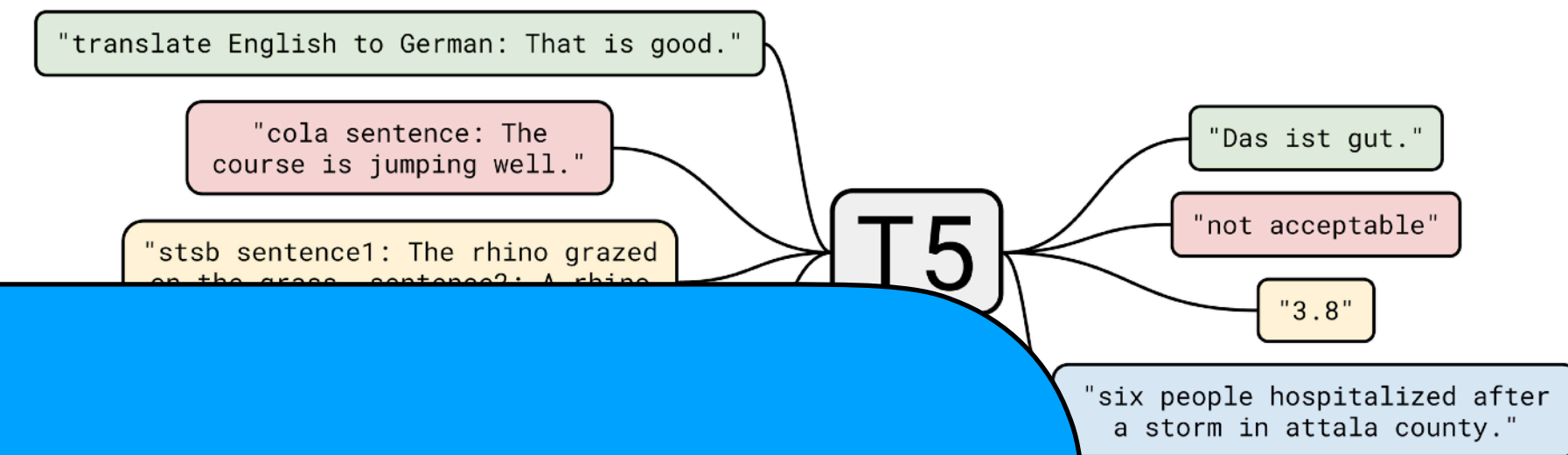
• Which privacy issues do users face?

- Allow gener...
- Quick...
- Add resear...
- Comp...



How to make privacy reviews digestible?

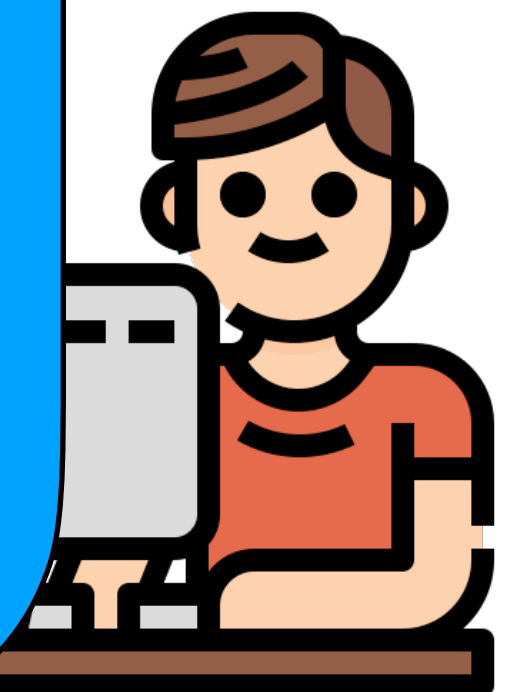
- Why not process this data with language models?



- Allow gener
- Quick
- Add resear
- Comp

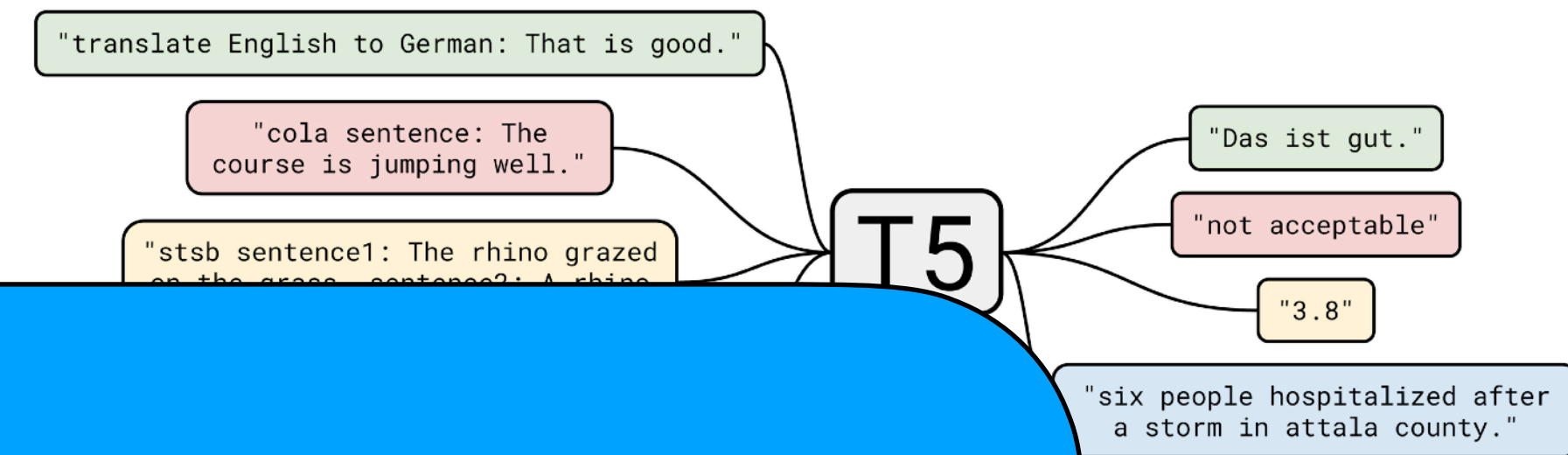
• Which privacy issues do users face?

• How do privacy issues evolve over time?



How to make privacy reviews digestible?

- Why not process this data with language models?



- Allow gener
- Quick
- Add resear
- Comp

• Which privacy issues do users face?

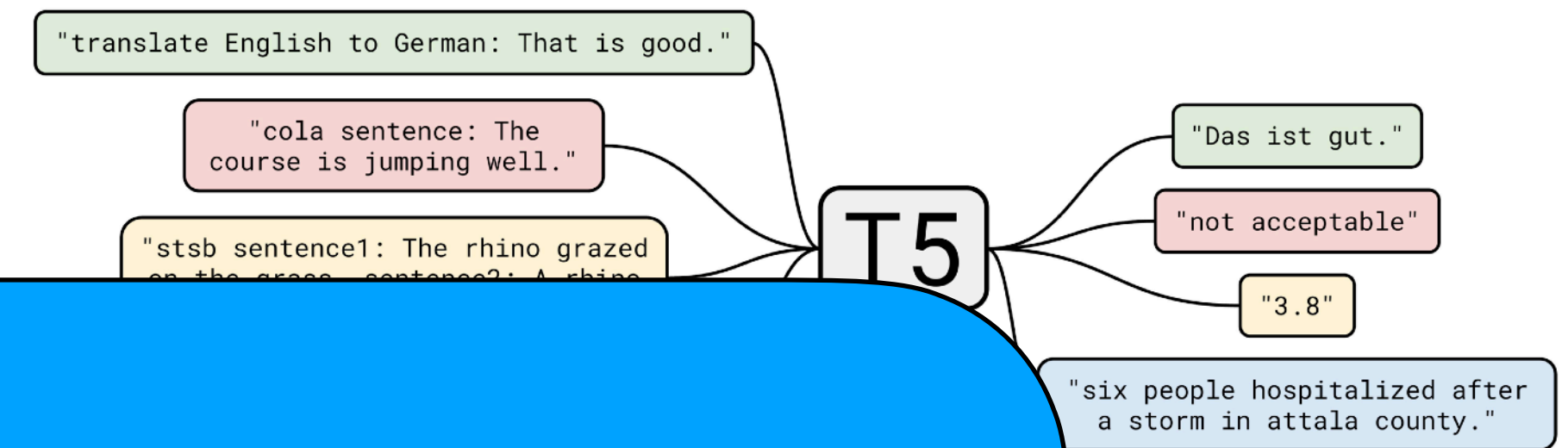
• How do privacy issues evolve over time?

• How do privacy issues vary across countries?



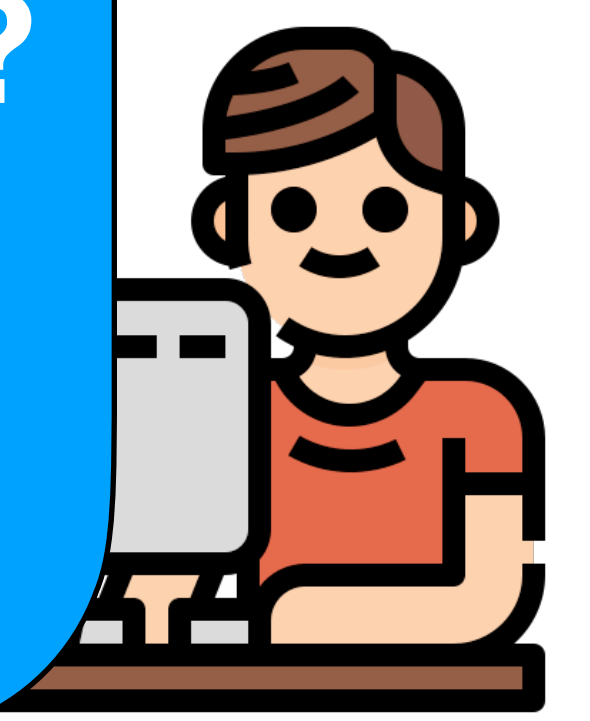
How to make privacy reviews digestible?

- Why not process this data with language models?



- Allow gener
- Quick
- Add rese
- Comp

- Which privacy issues do users face?
- How do privacy issues evolve over time?
- How do privacy issues vary across countries?
- How do privacy issues vary across products?



How to make privacy reviews digestible?

2022 IEEE Symposium on Security and Privacy (SP)

Hark: A Deep Learning System for Navigating Privacy Feedback at Scale

Hamza Harkous[‡], Sai Teja Peddinti[‡], Rishabh Khandelwal^{†*}, Animesh Srivastava[‡], and Nina Taft[‡]

[‡]Google, [†]University of Wisconsin-Madison

[‡]{harkous, psajteja, sranimesh, ninataft}@google.com, [†]rkhandelwal3@wisc.edu

Abstract—Integrating user feedback is one of the pillars for building successful products. However, this feedback is generally collected in an unstructured free-text form, which is challenging to understand at scale. This is particularly demanding in the privacy domain due to the nuances associated with the concept and the limited existing solutions. In this work, we present Hark¹, a system for discovering and summarizing privacy-related feedback at scale. Hark automates the entire process of summarizing privacy feedback, starting from unstructured text and resulting in a hierarchy of high-level privacy themes and fine-grained issues within each theme, along with representative reviews for each issue. At the core of Hark is a set of new deep learning models trained on different tasks, such as privacy feedback classification, privacy issues generation, and high-level theme creation. We illustrate Hark’s efficacy on a corpus of 626M Google Play reviews. Out of this corpus, our privacy feedback classifier extracts 6M privacy-related reviews (with an AUC-ROC of 0.92). With three annotation studies, we show that Hark’s generated issues are of high accuracy and coverage and that the theme titles are of high quality. We illustrate Hark’s capabilities by presenting high-level insights from 1.3M Android apps.

Previous attempts at analyzing privacy reviews [5, 7, 32, 34] have not built classifiers with *topical diversity* as a goal. They primarily relied on keyword-based sampling of training data, thus restricting the privacy issues users discuss to a set of predefined wordings. Moreover, these approaches did not go further beyond the classification step. Hence, they fail at creating a structure out of the reviews. Even when considering the broader work on analyzing app reviews [11, 18, 36], we notice that these fall short at providing *glanceable* summaries of the topics users raise. They are often restricted to extracting verbatim keywords or phrases from users’ reviews [11]. The ultimate result achieved there is a set of clustered reviews, without an explainable common theme for each cluster. This results in a lot of manual work for *navigating* through reviews by reading them, finding issues users discuss, and understanding the high-level themes summarizing users’ privacy feedback.

Despite these shortcomings, previous works have shown that, when developers are made aware of privacy reviews, they do carry out related updates [24]. Similar results were

How to make privacy reviews digestible?

2022 IEEE Symposium on Security and Privacy (SP)

Hark! Deep Learning System for Navigating Privacy Feedback at Scale

Hamza Harkous[‡], Sai Teja Peddinti[‡], Rishabh Khandelwal^{†*}, Animesh Srivastava[‡], and Nina Taft[‡]

[‡]Google, [†]University of Wisconsin-Madison

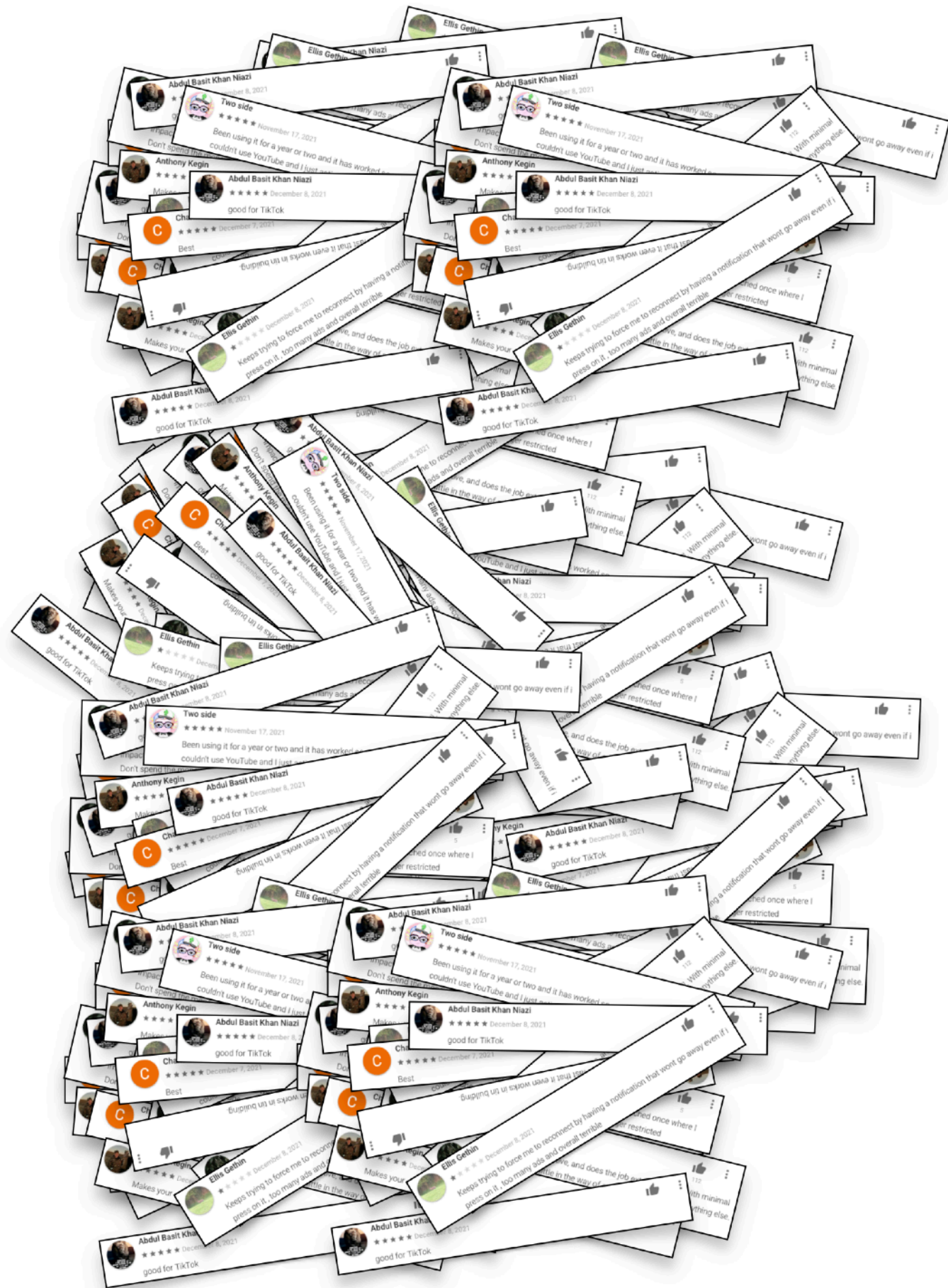
[‡]{harkous, psajteja, sranimesh, ninataft}@google.com, [†]rkhandelwal3@wisc.edu

Abstract—Integrating user feedback is one of the pillars for building successful products. However, this feedback is generally collected in an unstructured free-text form, which is challenging to understand at scale. This is particularly demanding in the privacy domain due to the nuances associated with the concept and the limited existing solutions. In this work, we present Hark¹, a system for discovering and summarizing privacy-related feedback at scale. Hark automates the entire process of summarizing privacy feedback, starting from unstructured text and resulting in a hierarchy of high-level privacy themes and fine-grained issues within each theme, along with representative reviews for each issue. At the core of Hark is a set of new deep learning models trained on different tasks, such as privacy feedback classification, privacy issues generation, and high-level theme creation. We illustrate Hark's efficacy on a corpus of 626M Google Play reviews. Out of this corpus, our privacy feedback classifier extracts 6M privacy-related reviews (with an AUC-ROC of 0.92). With three annotation studies, we show that Hark's generated issues are of high accuracy and coverage and that the theme titles are of high quality. We illustrate Hark's capabilities by presenting high-level insights from 1.3M Android apps.

Previous attempts at analyzing privacy reviews [5, 7, 32, 34] have not built classifiers with *topical diversity* as a goal. They primarily relied on keyword-based sampling of training data, thus restricting the privacy issues users discuss to a set of predefined wordings. Moreover, these approaches did not go further beyond the classification step. Hence, they fail at creating a structure out of the reviews. Even when considering the broader work on analyzing app reviews [11, 18, 36], we notice that these fall short at providing *glanceable* summaries of the topics users raise. They are often restricted to extracting verbatim keywords or phrases from users' reviews [11]. The ultimate result achieved there is a set of clustered reviews, without an explainable common theme for each cluster. This results in a lot of manual work for *navigating* through reviews by reading them, finding issues users discuss, and understanding the high-level themes summarizing users' privacy feedback.

Despite these shortcomings, previous works have shown that, when developers are made aware of privacy reviews, they do carry out related updates [24]. Similar results where

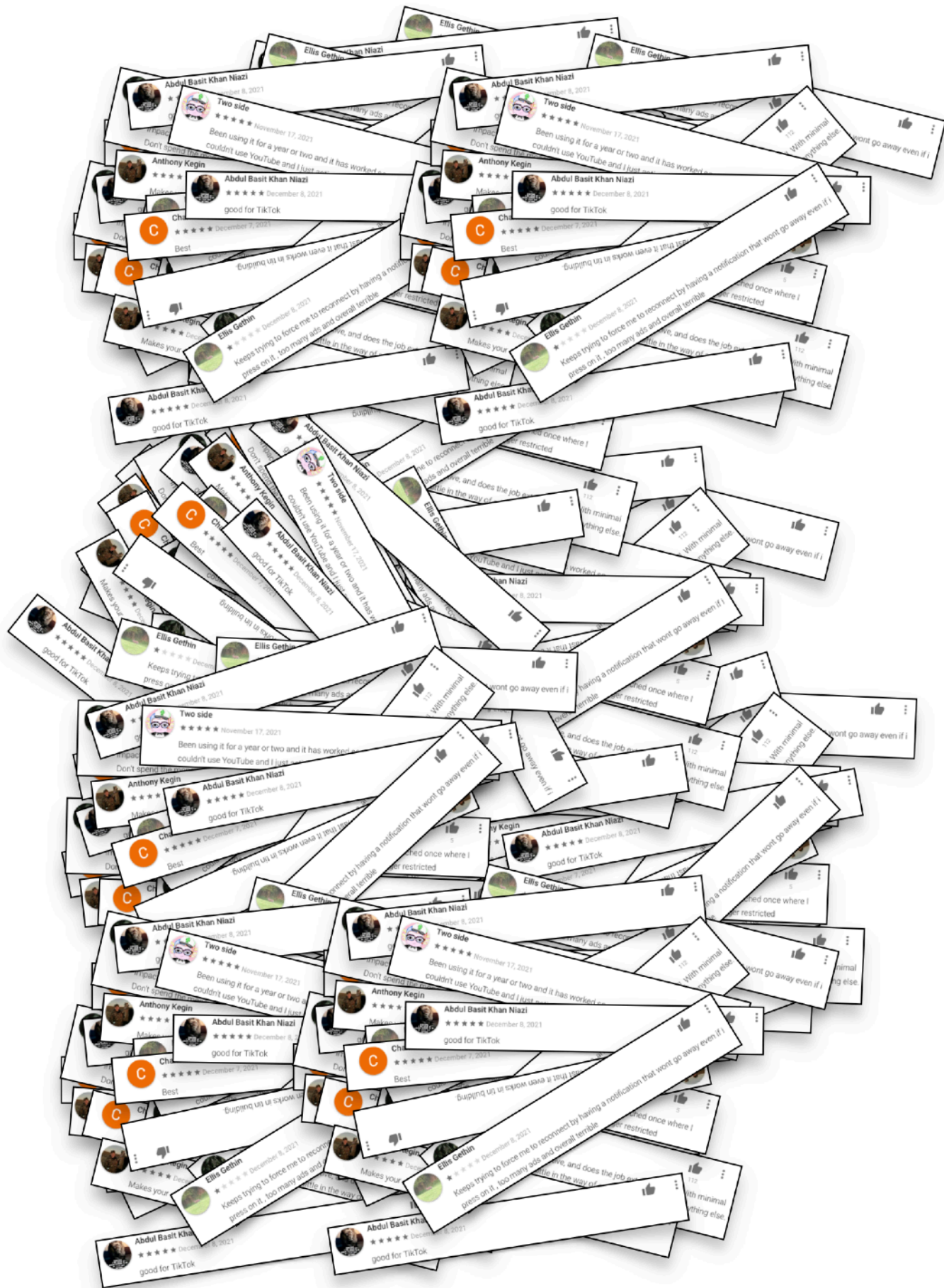
Our use: Analyze all Android app reviews!



**~2 billion
public reviews**

Our use: Analyze all Android app reviews!

Hark!+

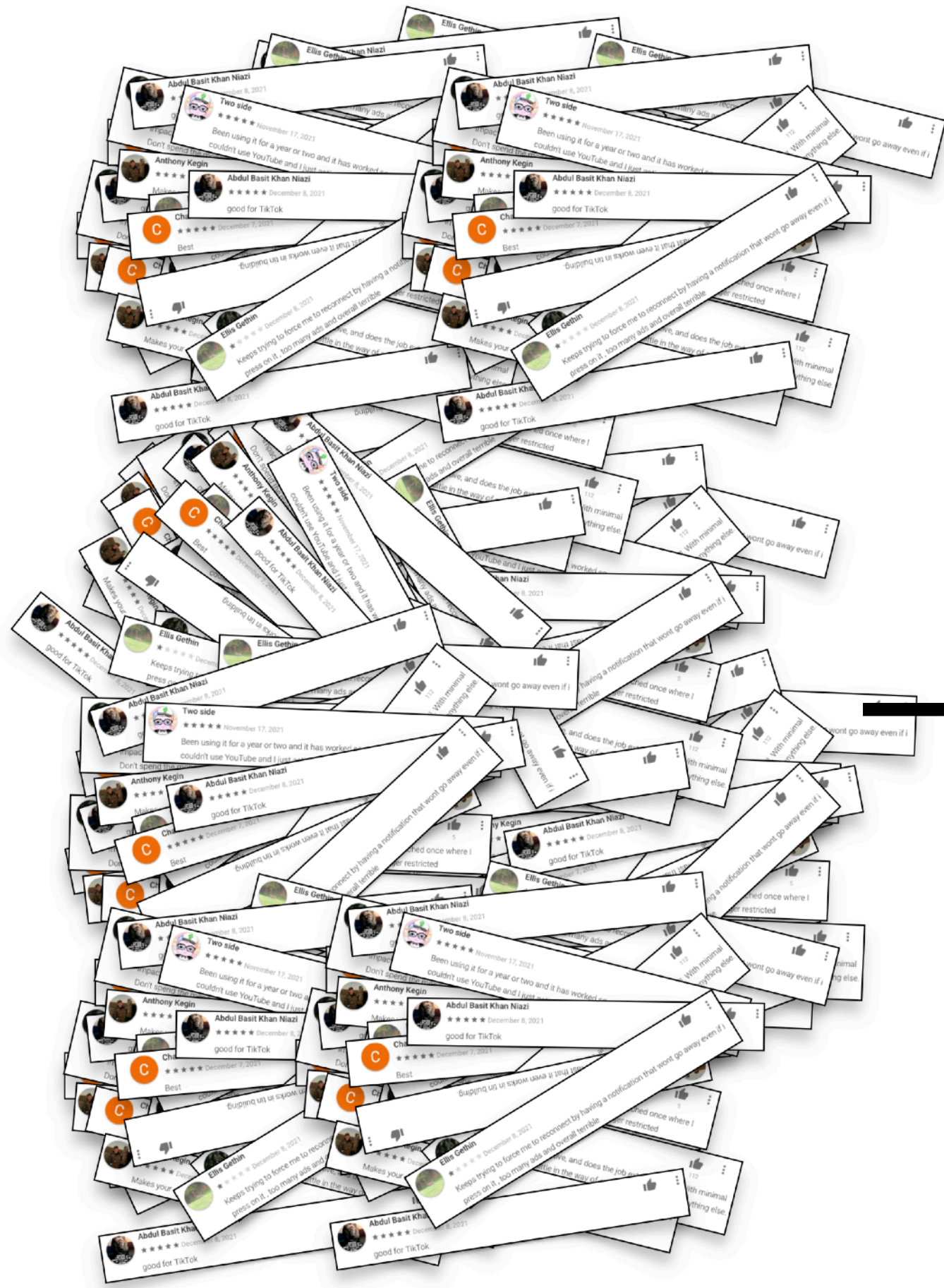


**~2 billion
public reviews**

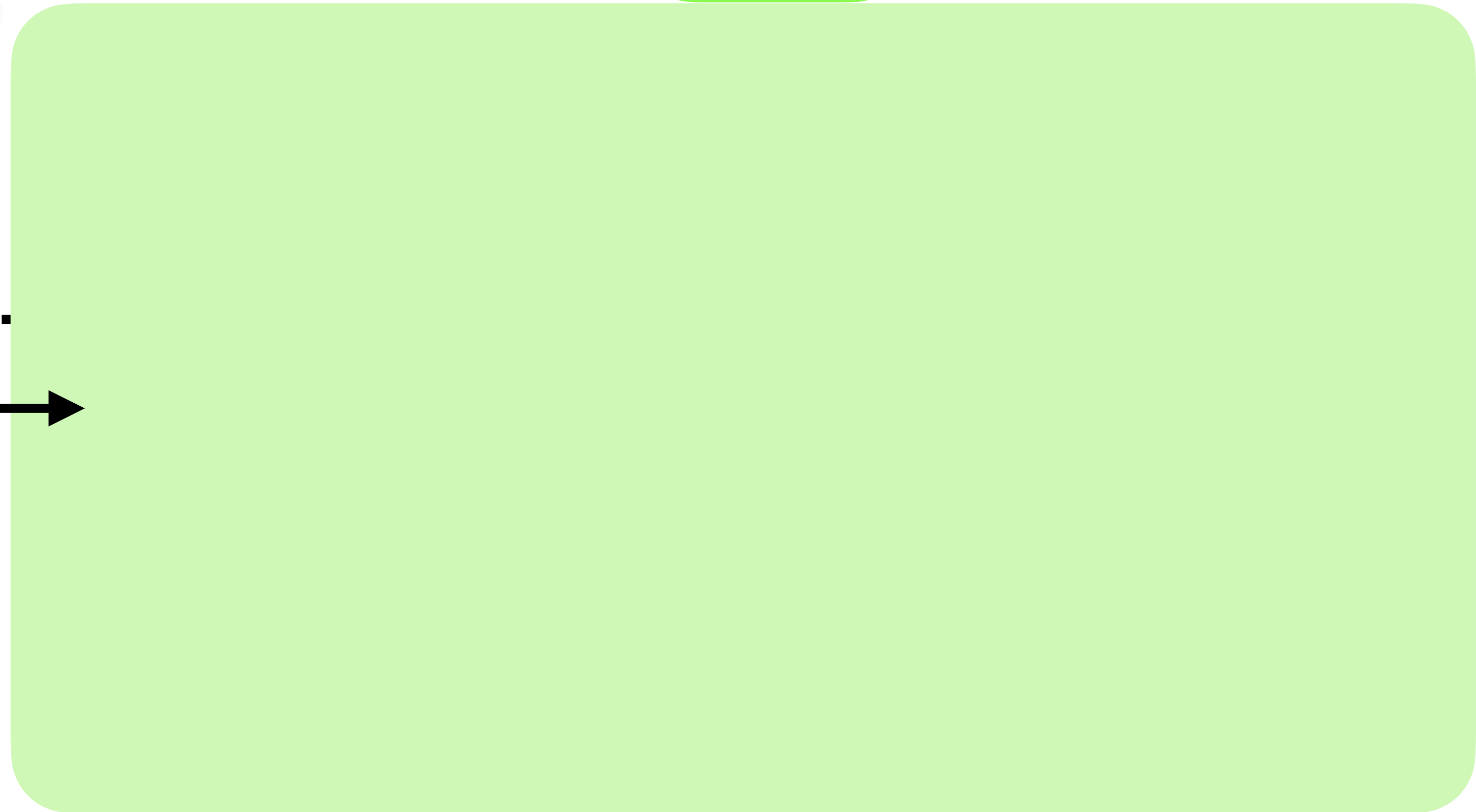
Some resources from play.google.com

Our use: Analyze all Android app reviews!

Hark!+

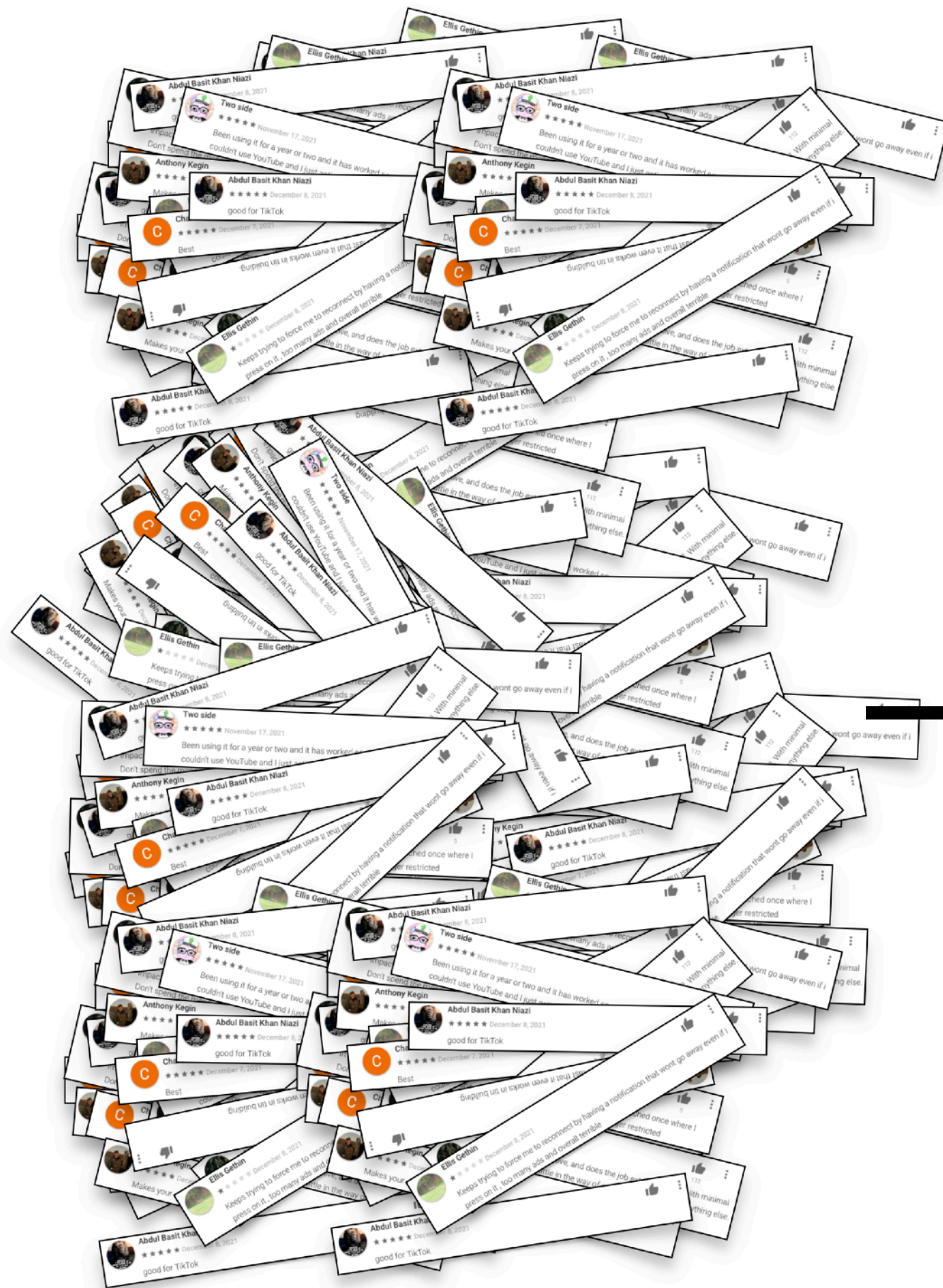


**~2 billion
public reviews**



Our use: Analyze all Android app reviews!

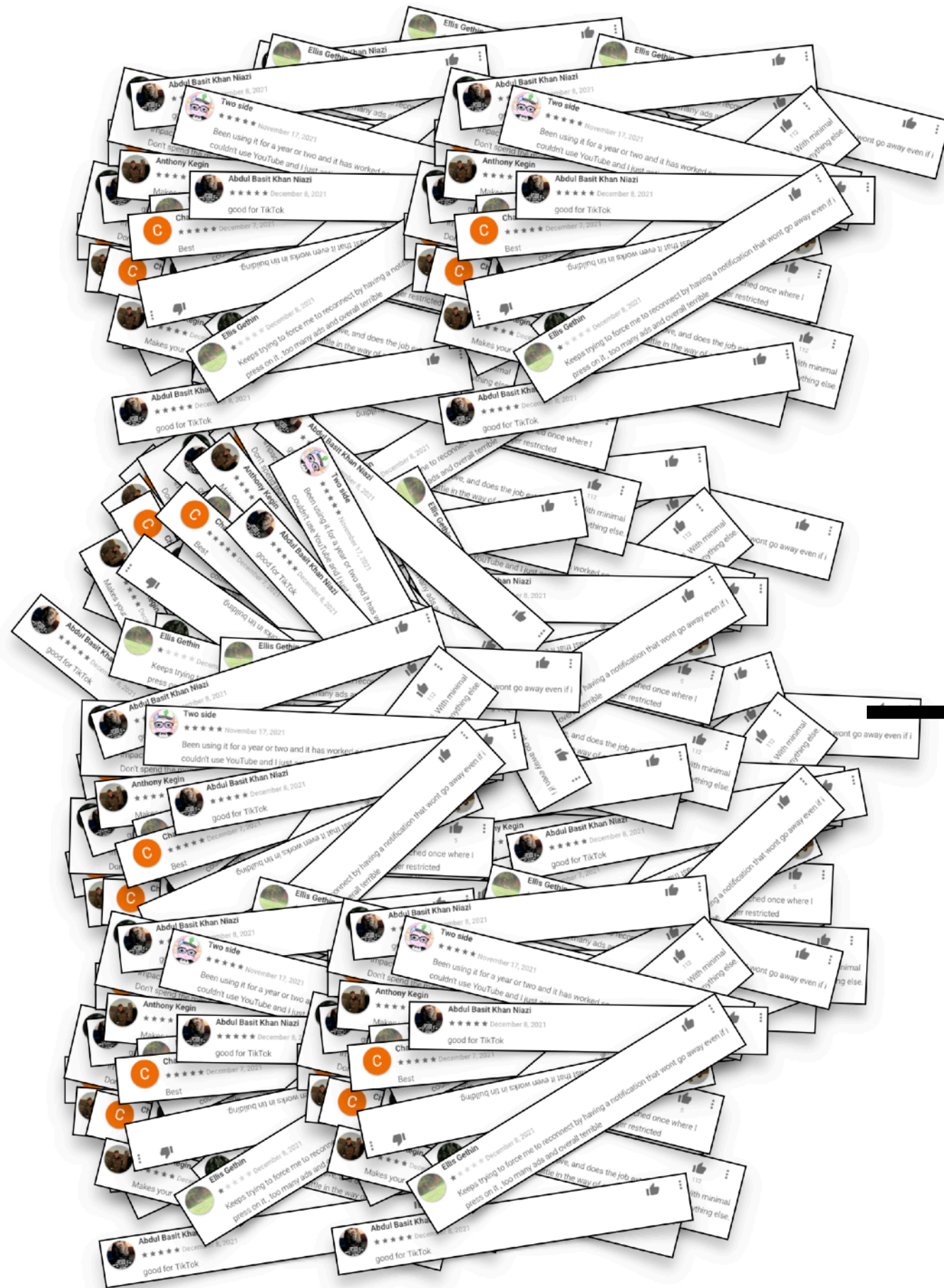
Hark!⁺



**~2 billion
public reviews**

Our use: Analyze all Android app reviews!

Hark!+

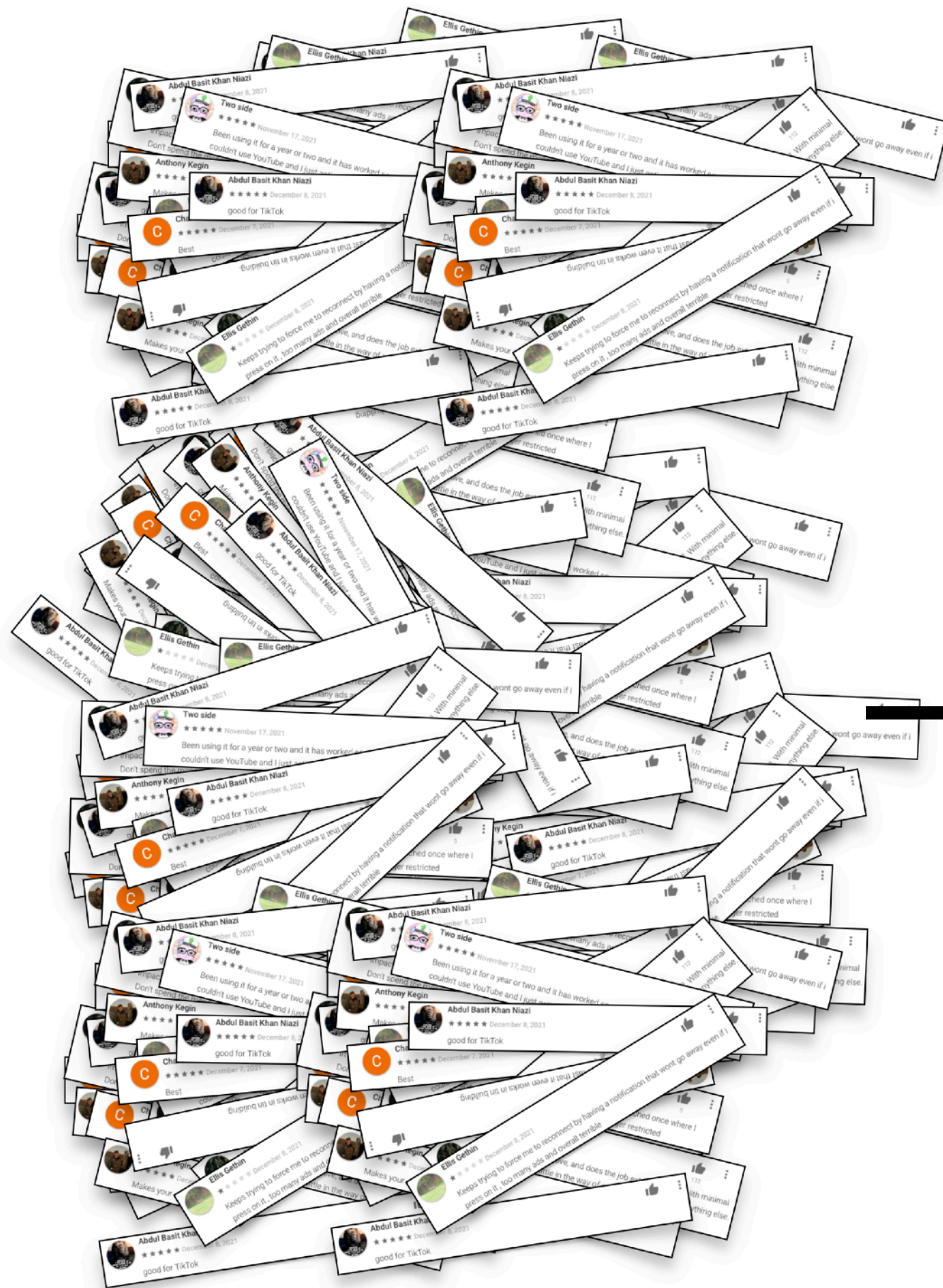


~2 billion
public reviews

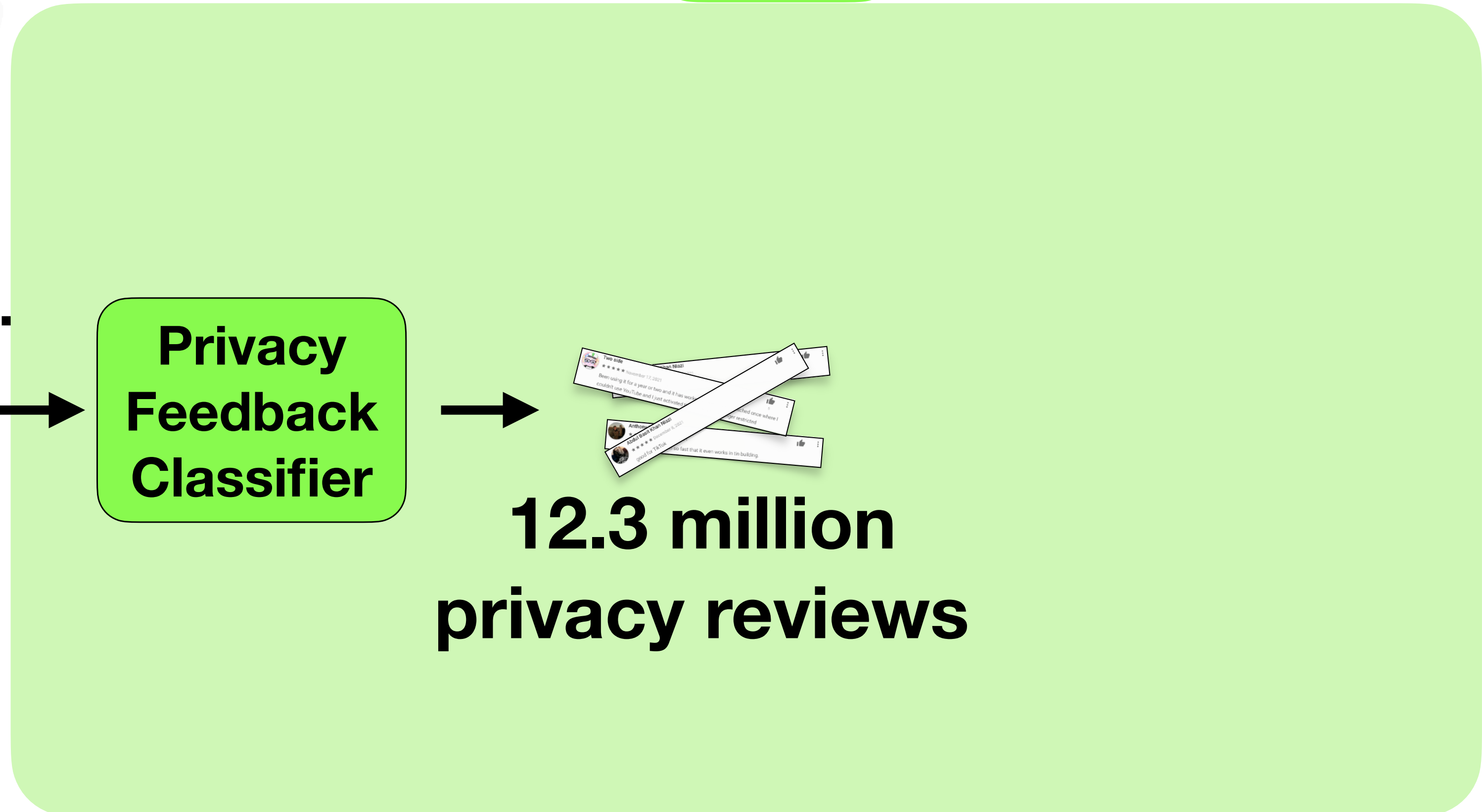
Privacy
Feedback
Classifier

Our use: Analyze all Android app reviews!

Hark!⁺



**~2 billion
public reviews**

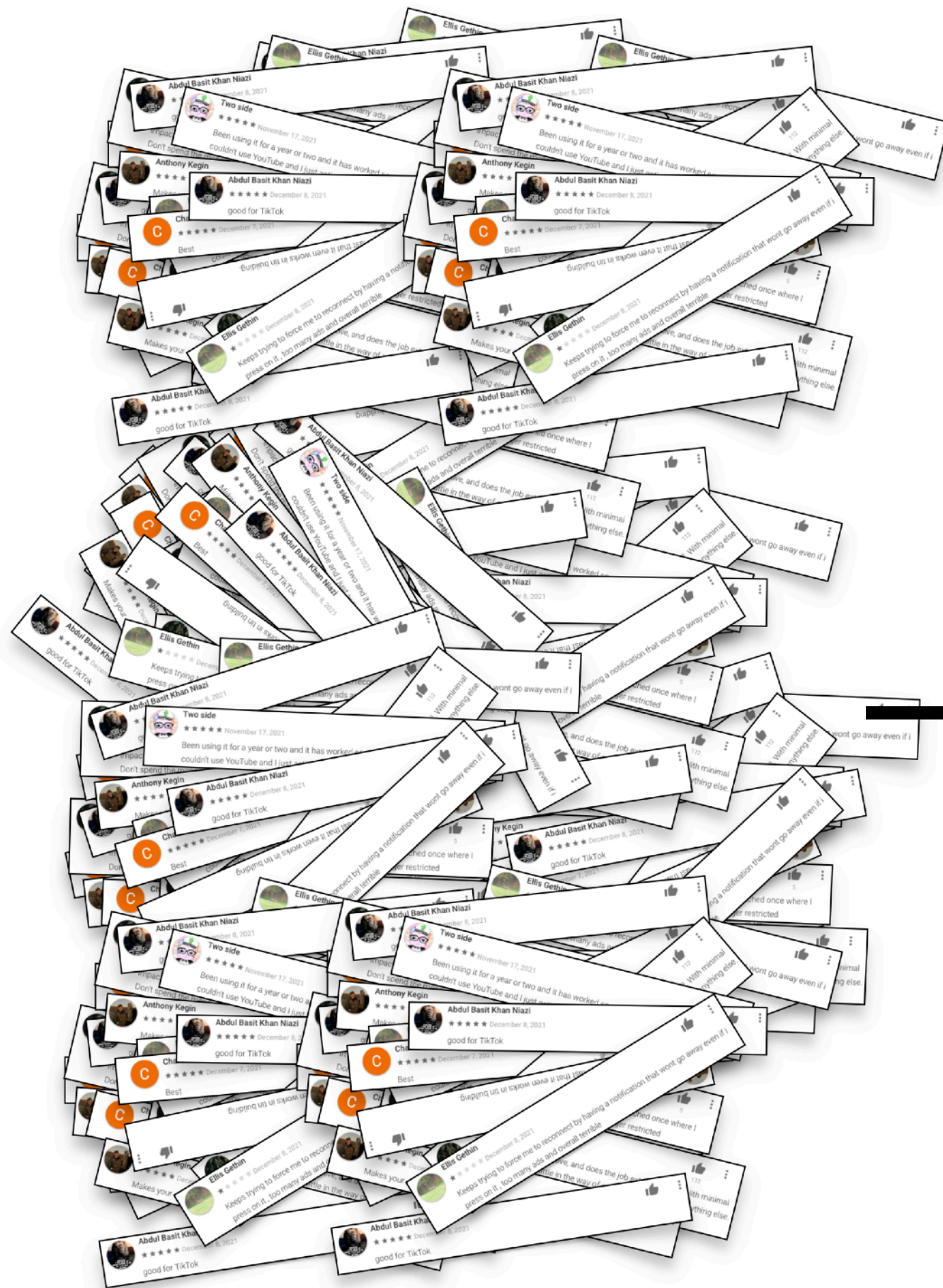


**Privacy
Feedback
Classifier**

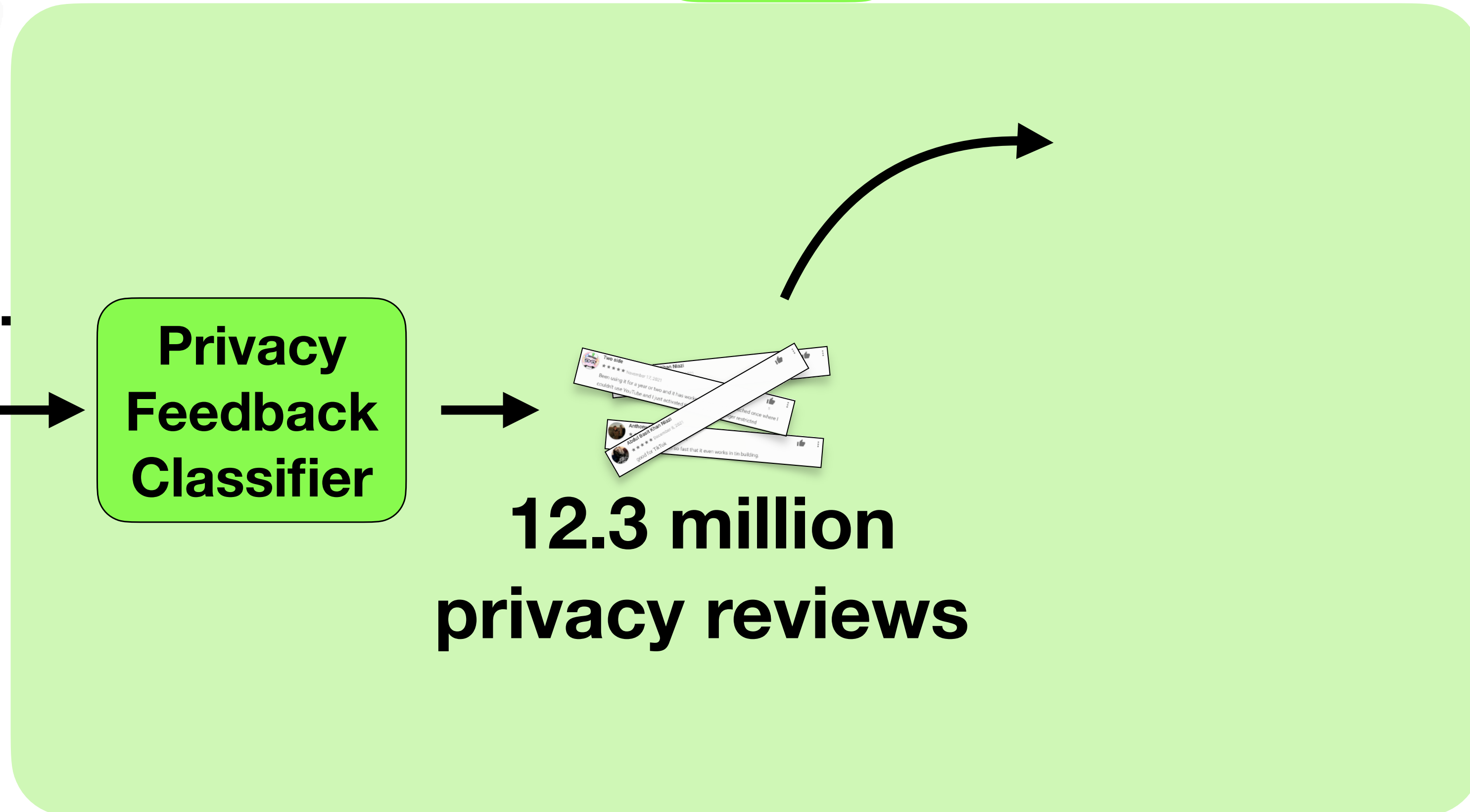
**12.3 million
privacy reviews**

Our use: Analyze all Android app reviews!

Hark!⁺

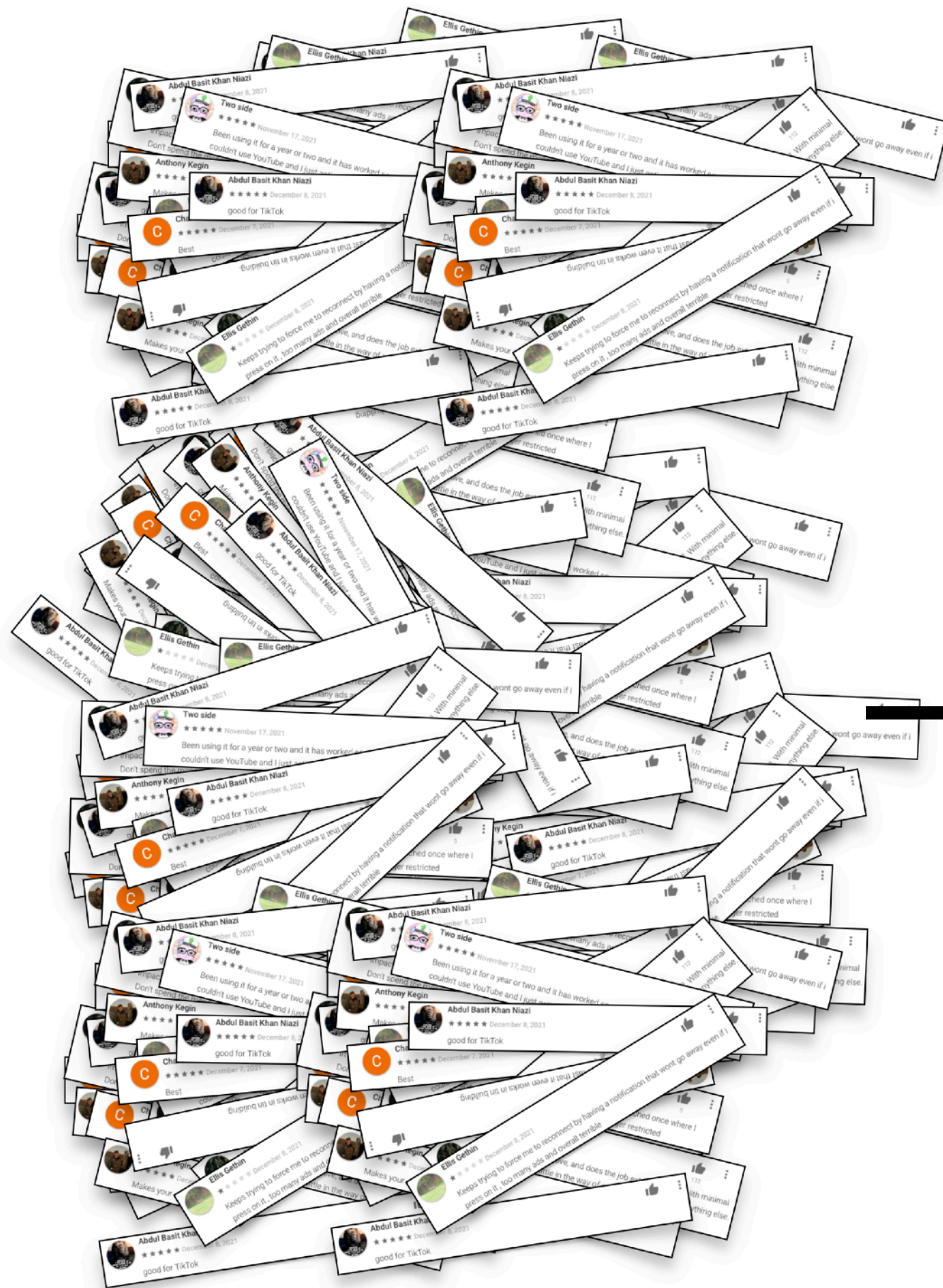


**~2 billion
public reviews**

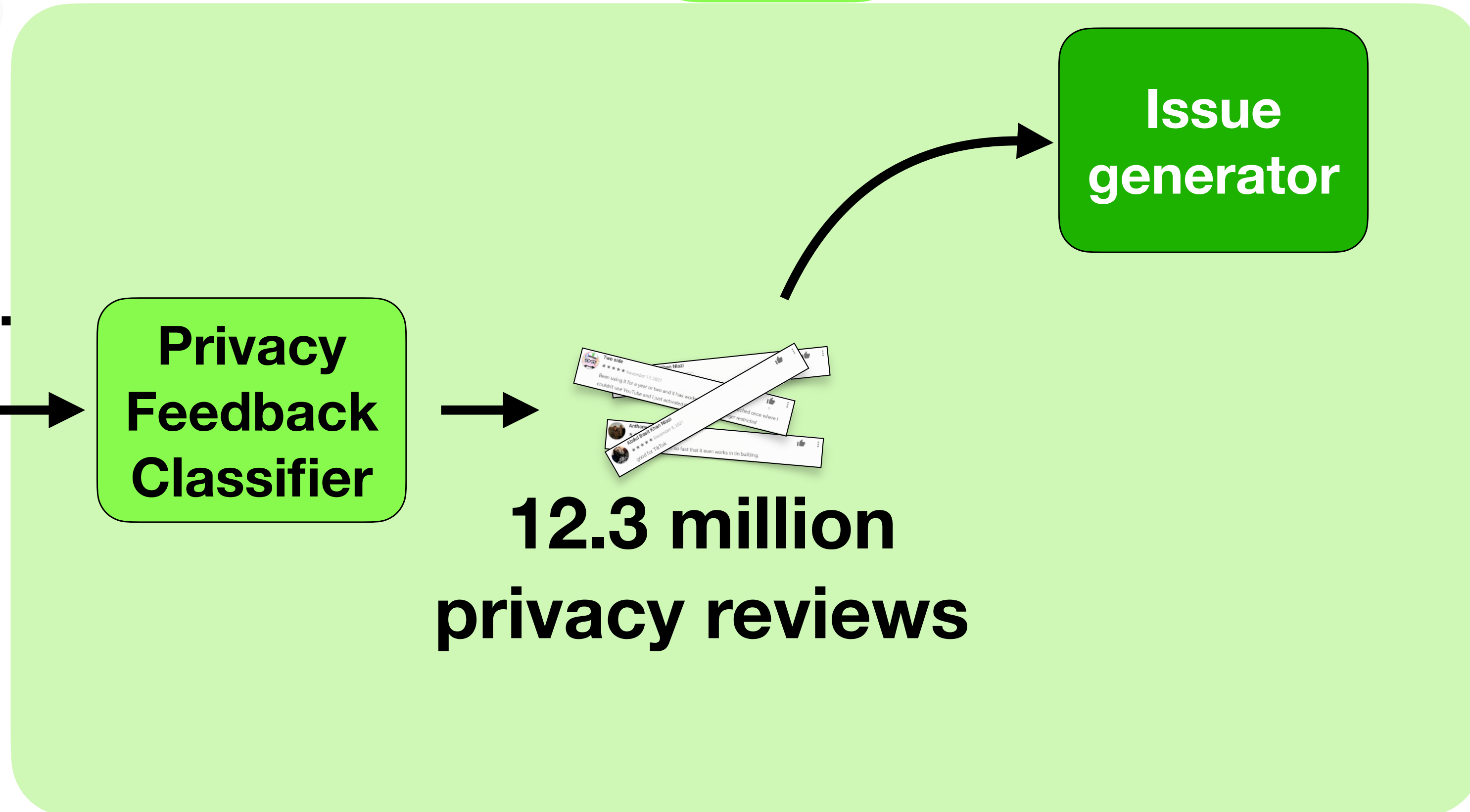


Our use: Analyze all Android app reviews!

Hark!⁺

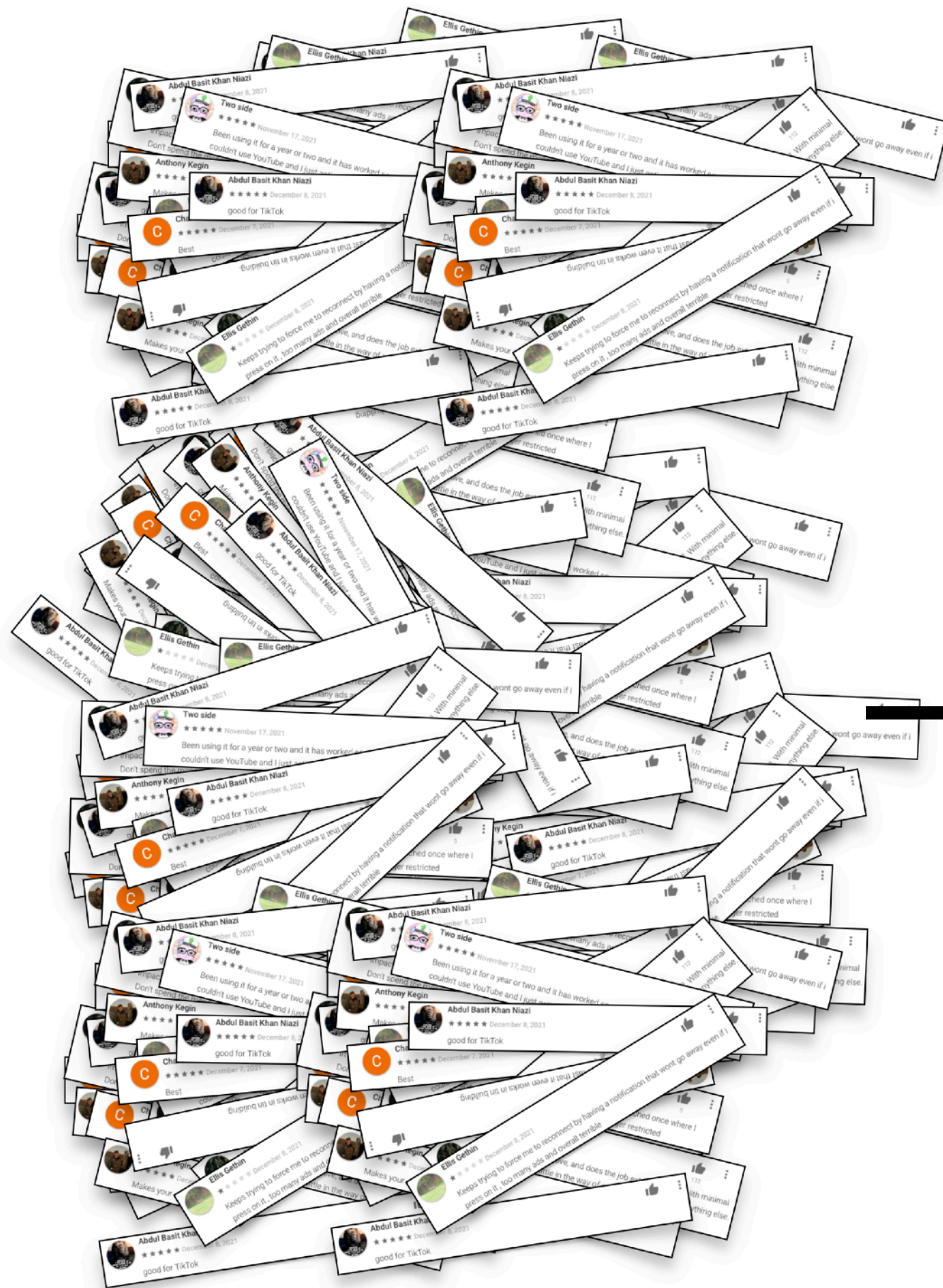


**~2 billion
public reviews**

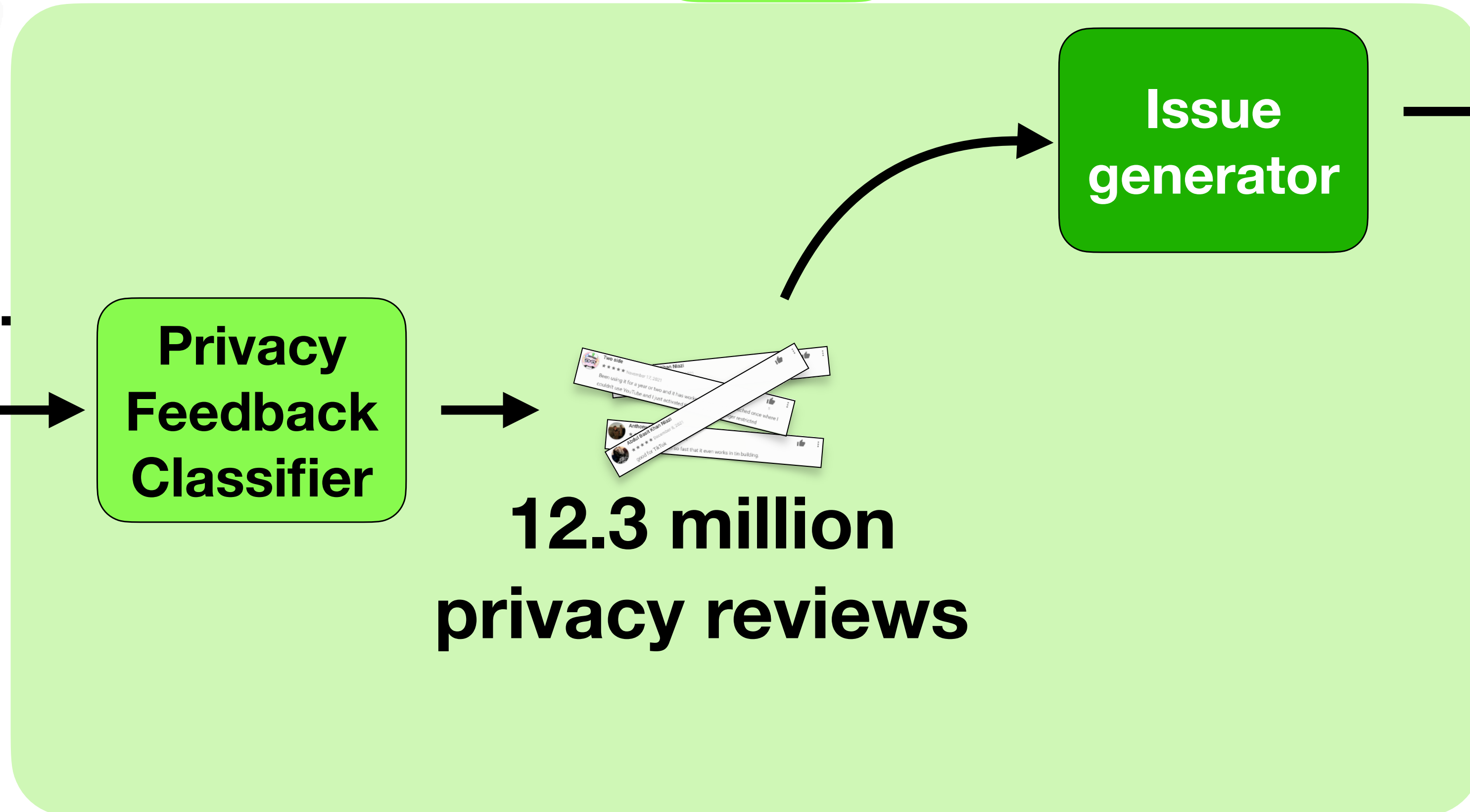


Our use: Analyze all Android app reviews!

Hark!⁺

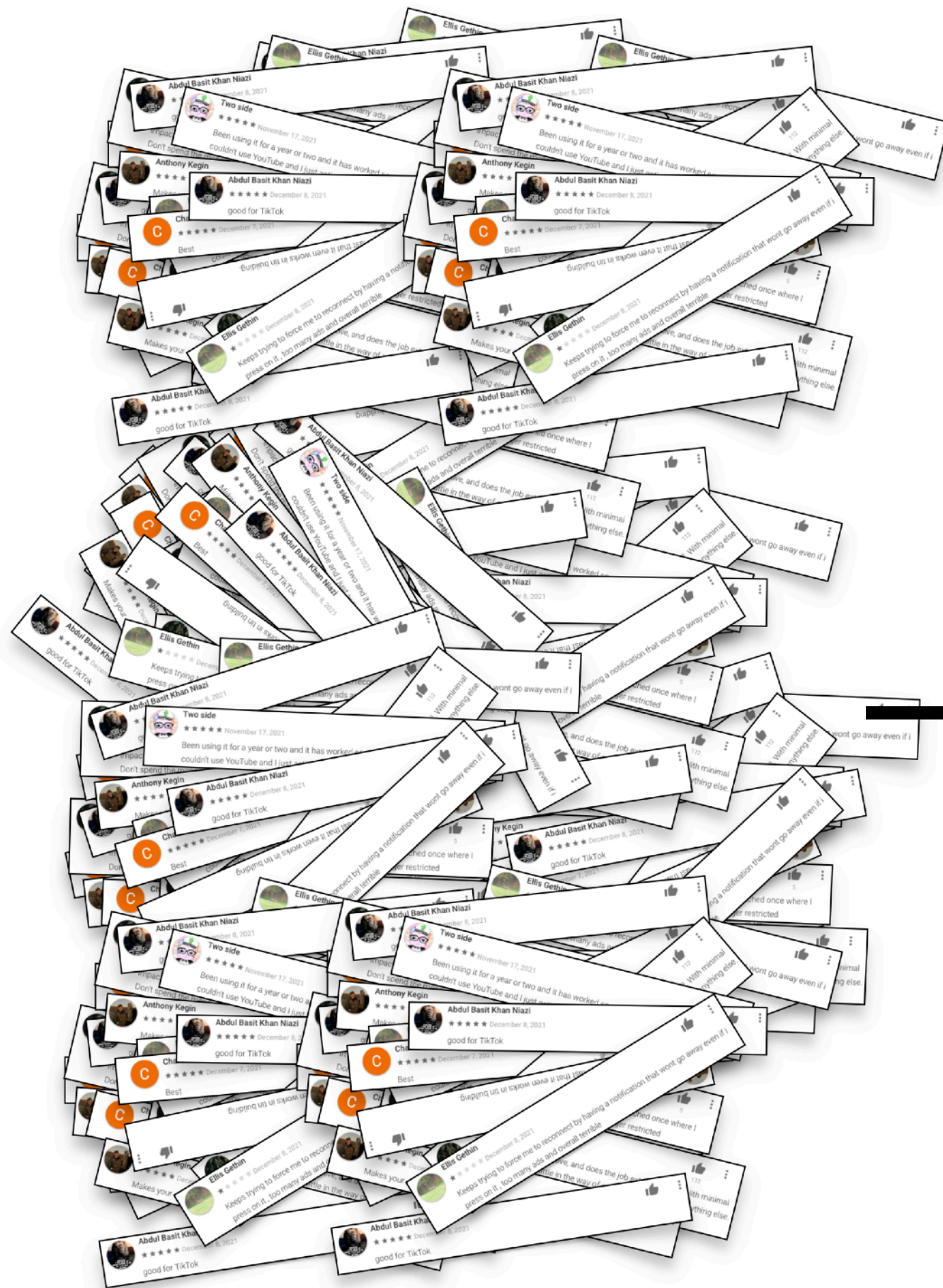


**~2 billion
public reviews**

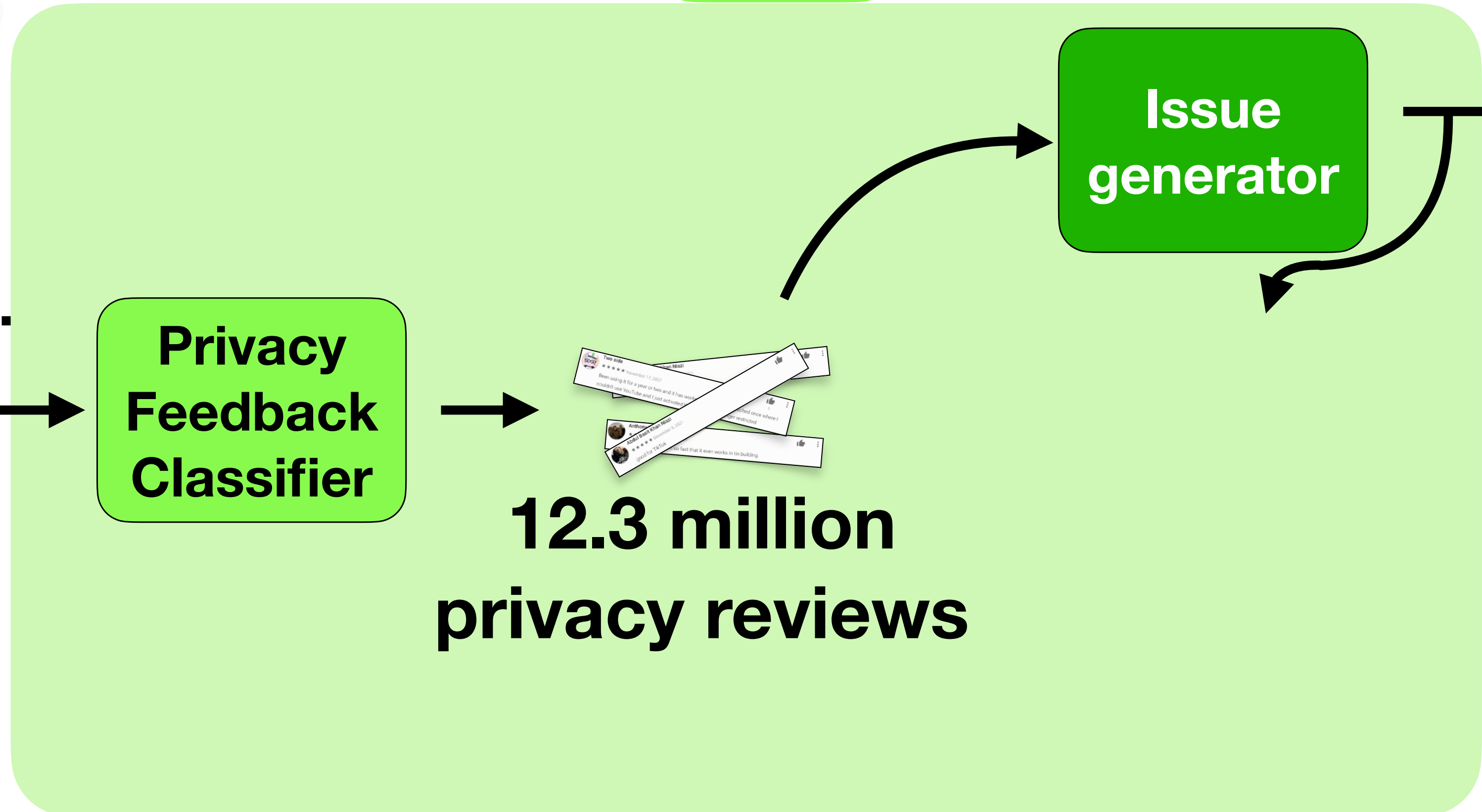


Our use: Analyze all Android app reviews!

Hark!+

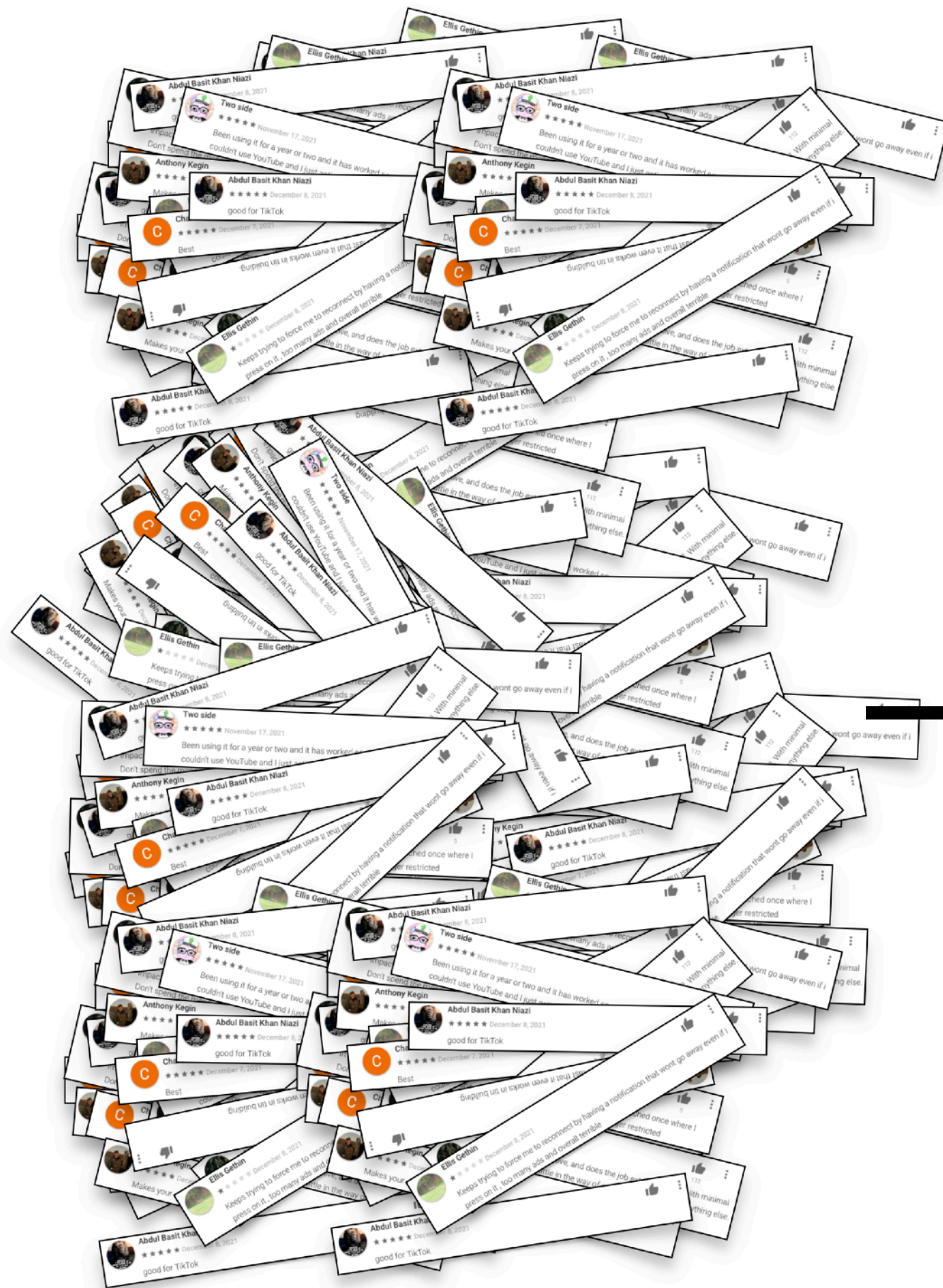


**~2 billion
public reviews**

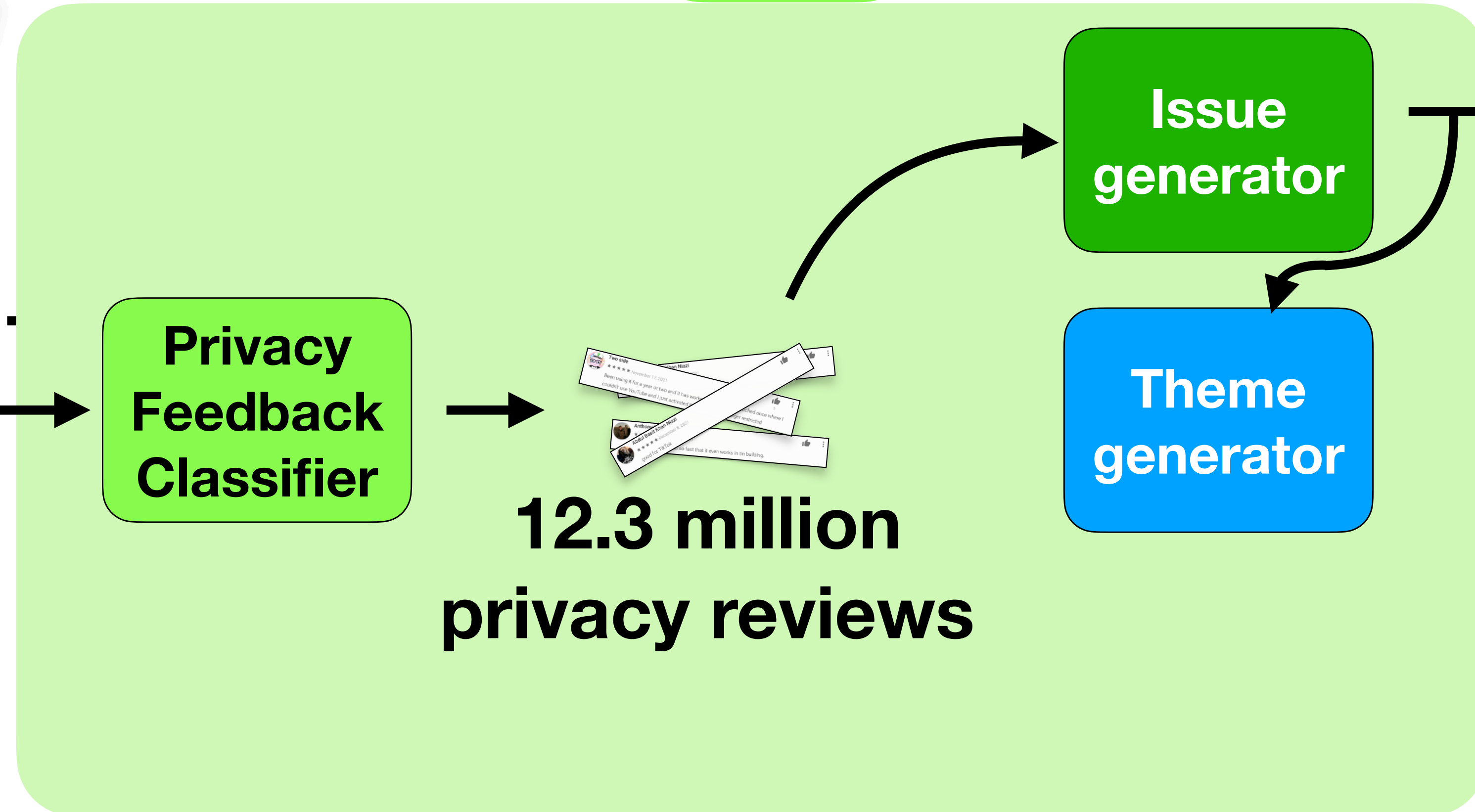


Our use: Analyze all Android app reviews!

Hark!+

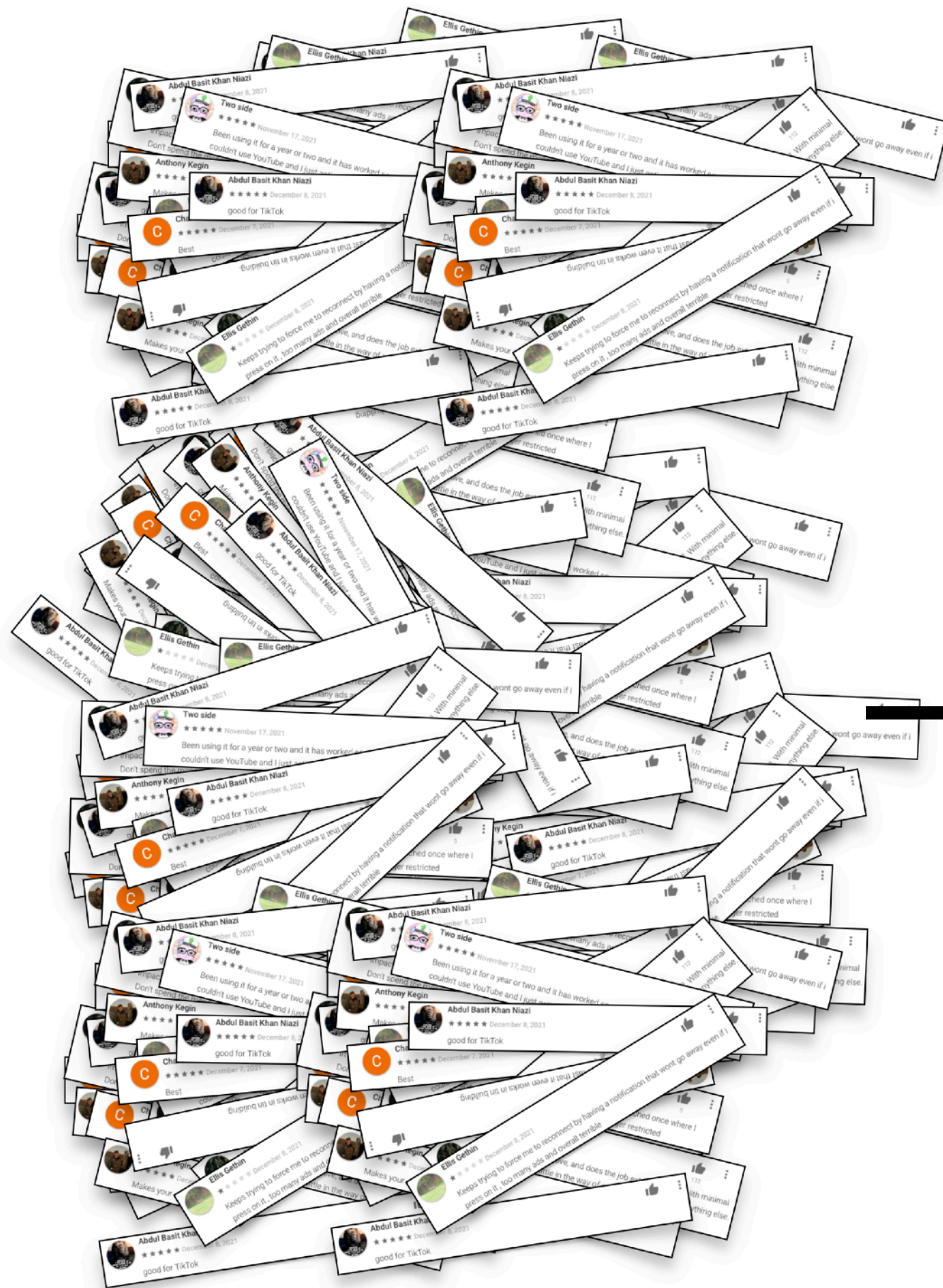


**~2 billion
public reviews**

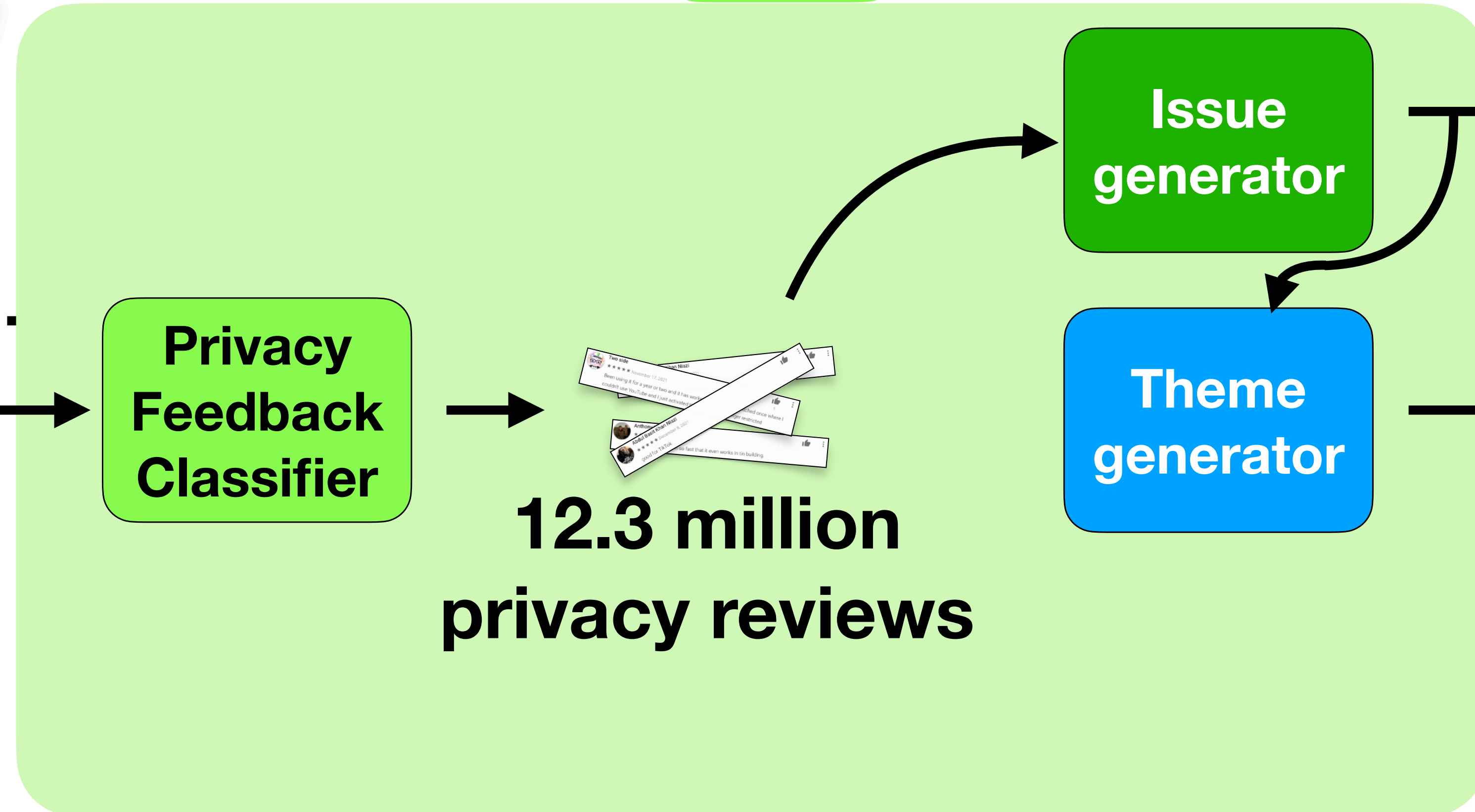


Our use: Analyze all Android app reviews!

Hark!+

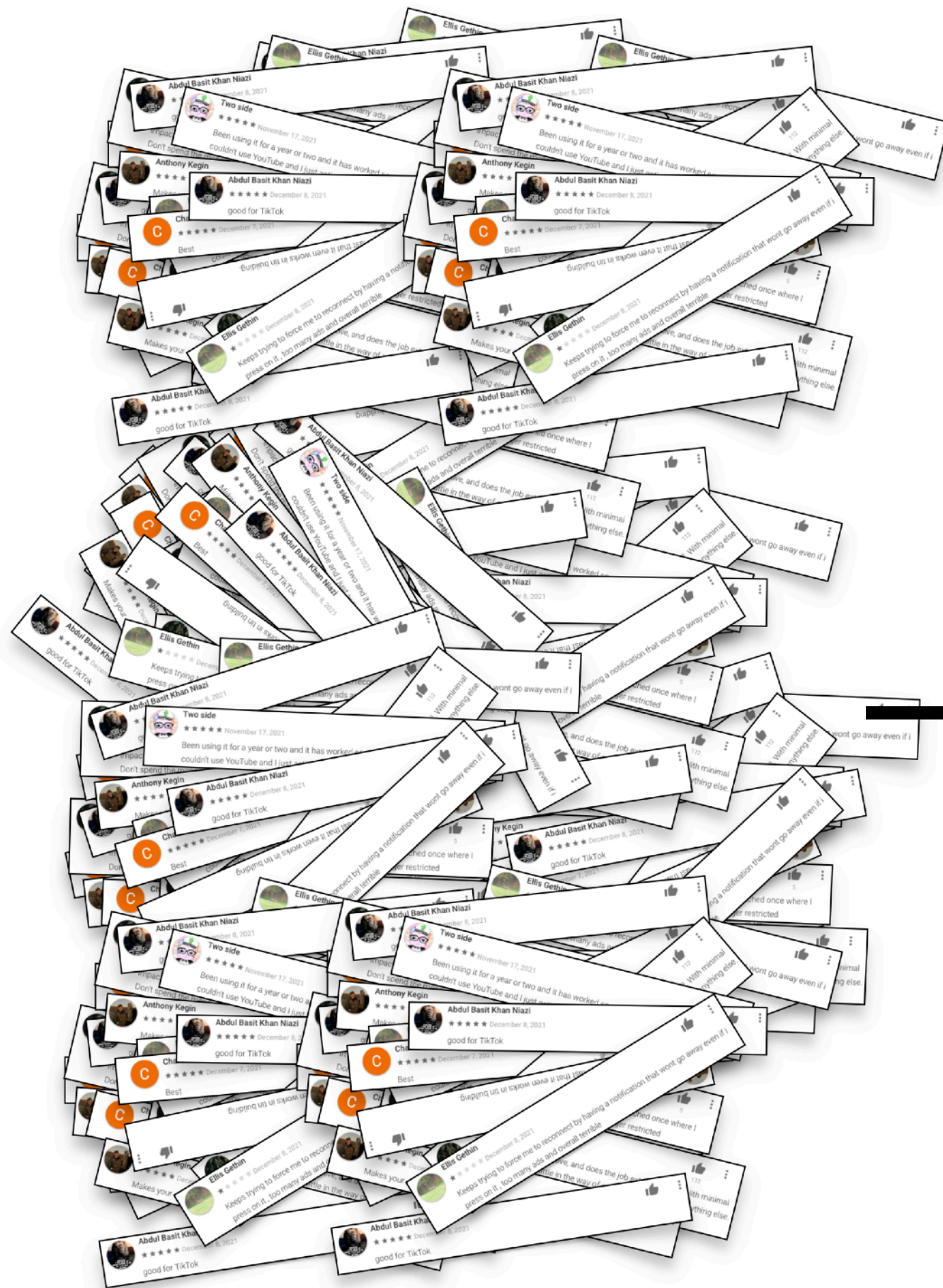


**~2 billion
public reviews**

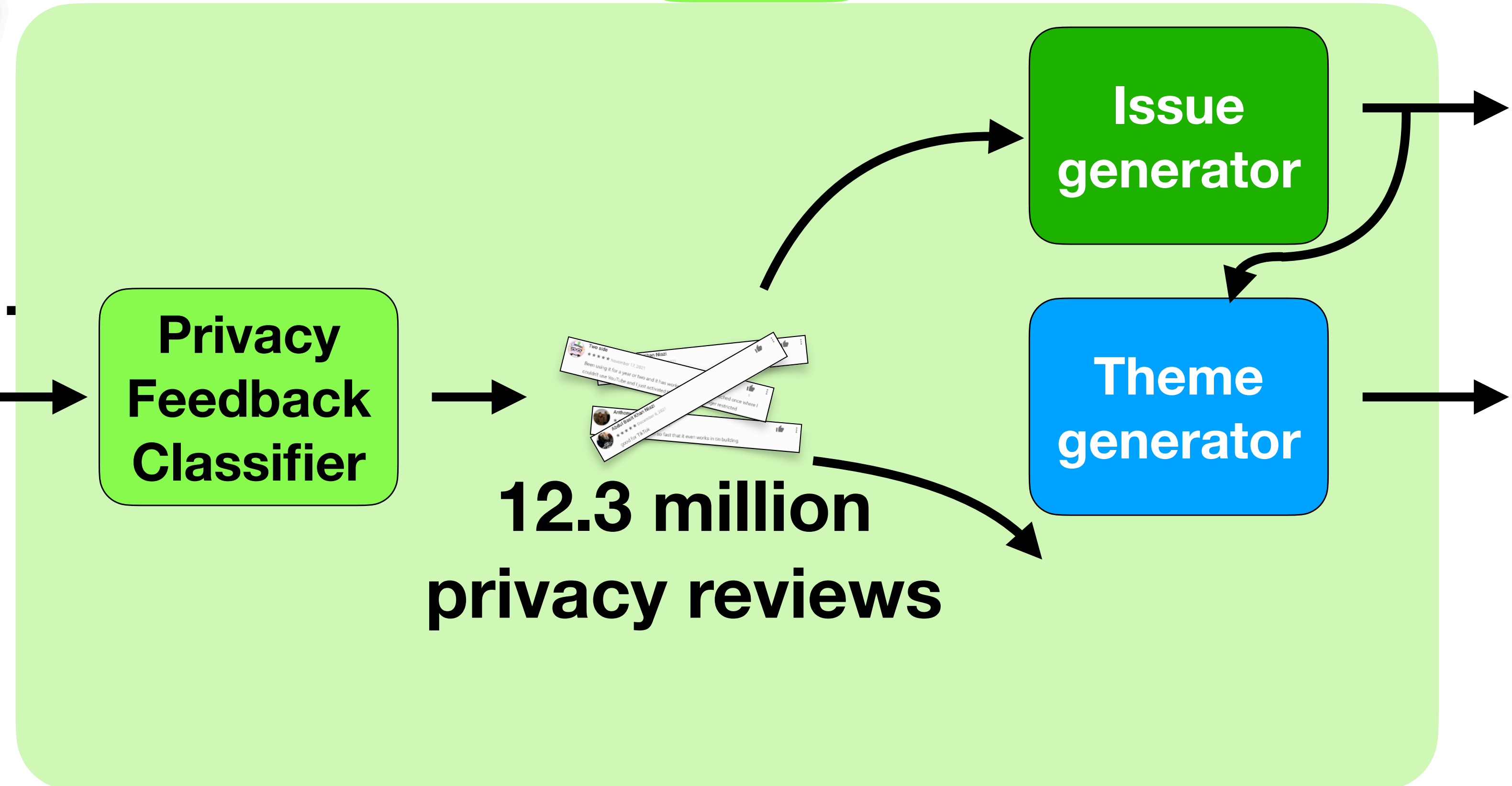


Our use: Analyze all Android app reviews!

Hark!⁺

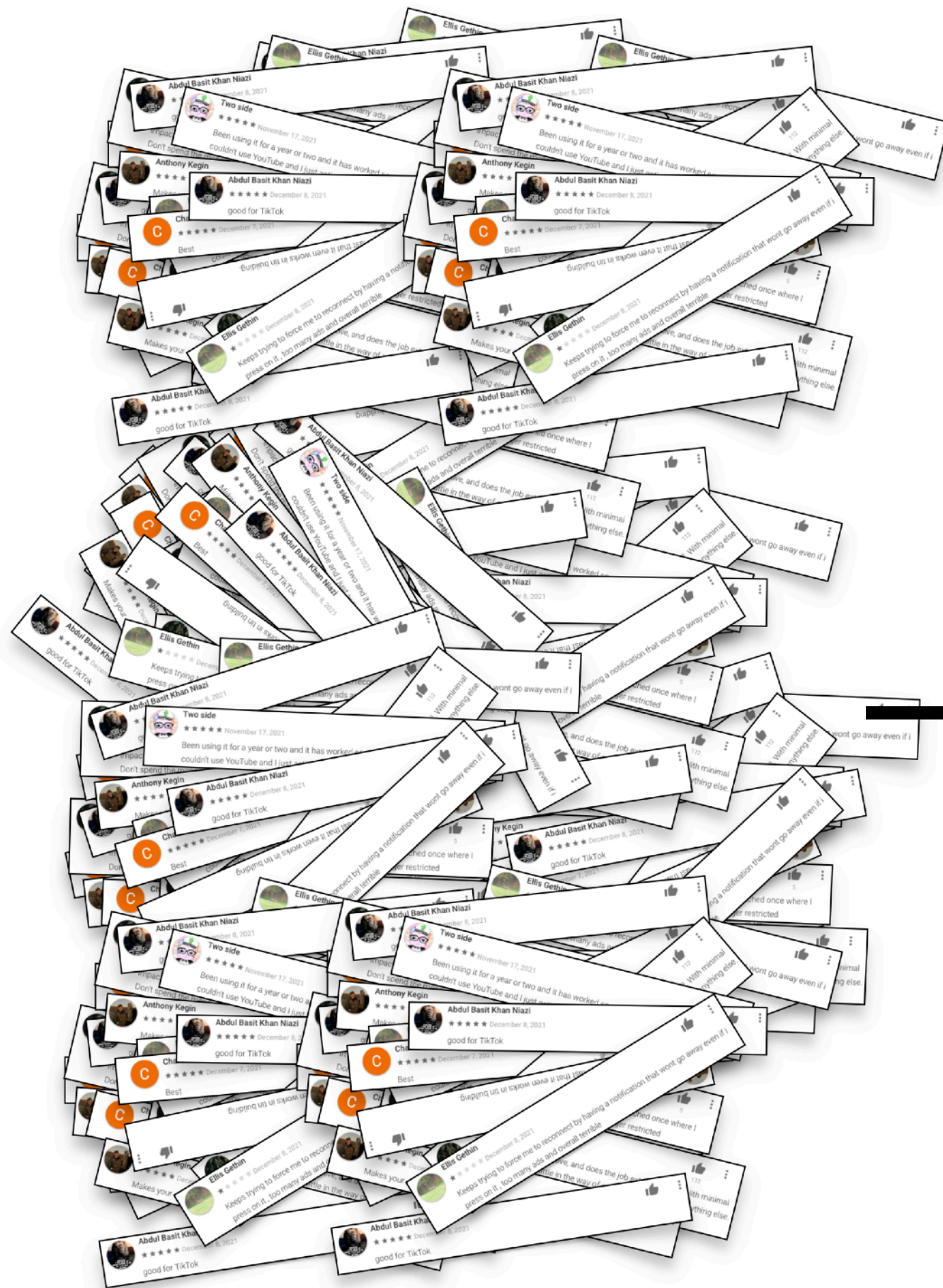


**~2 billion
public reviews**

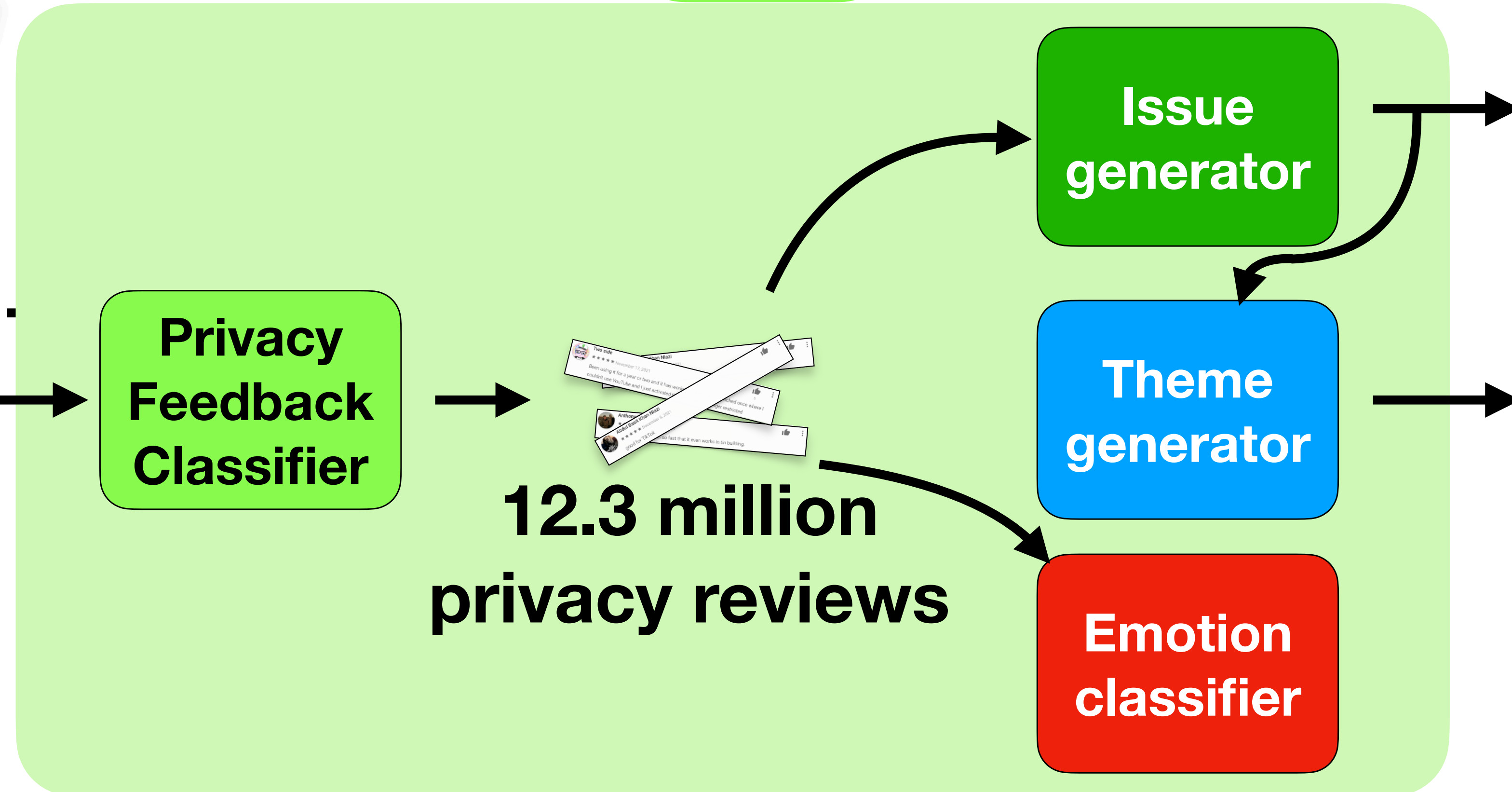


Our use: Analyze all Android app reviews!

Hark!⁺

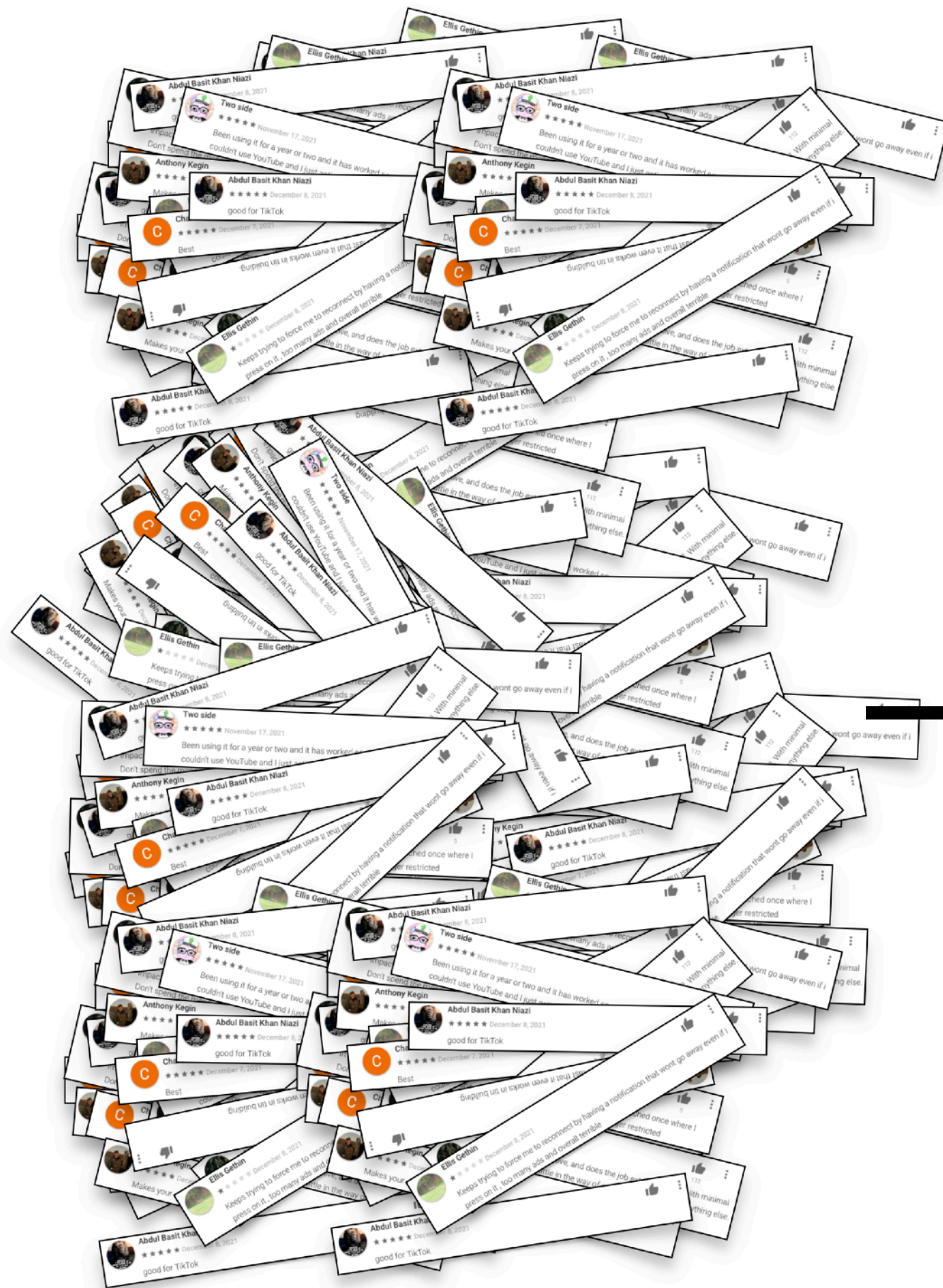


**~2 billion
public reviews**

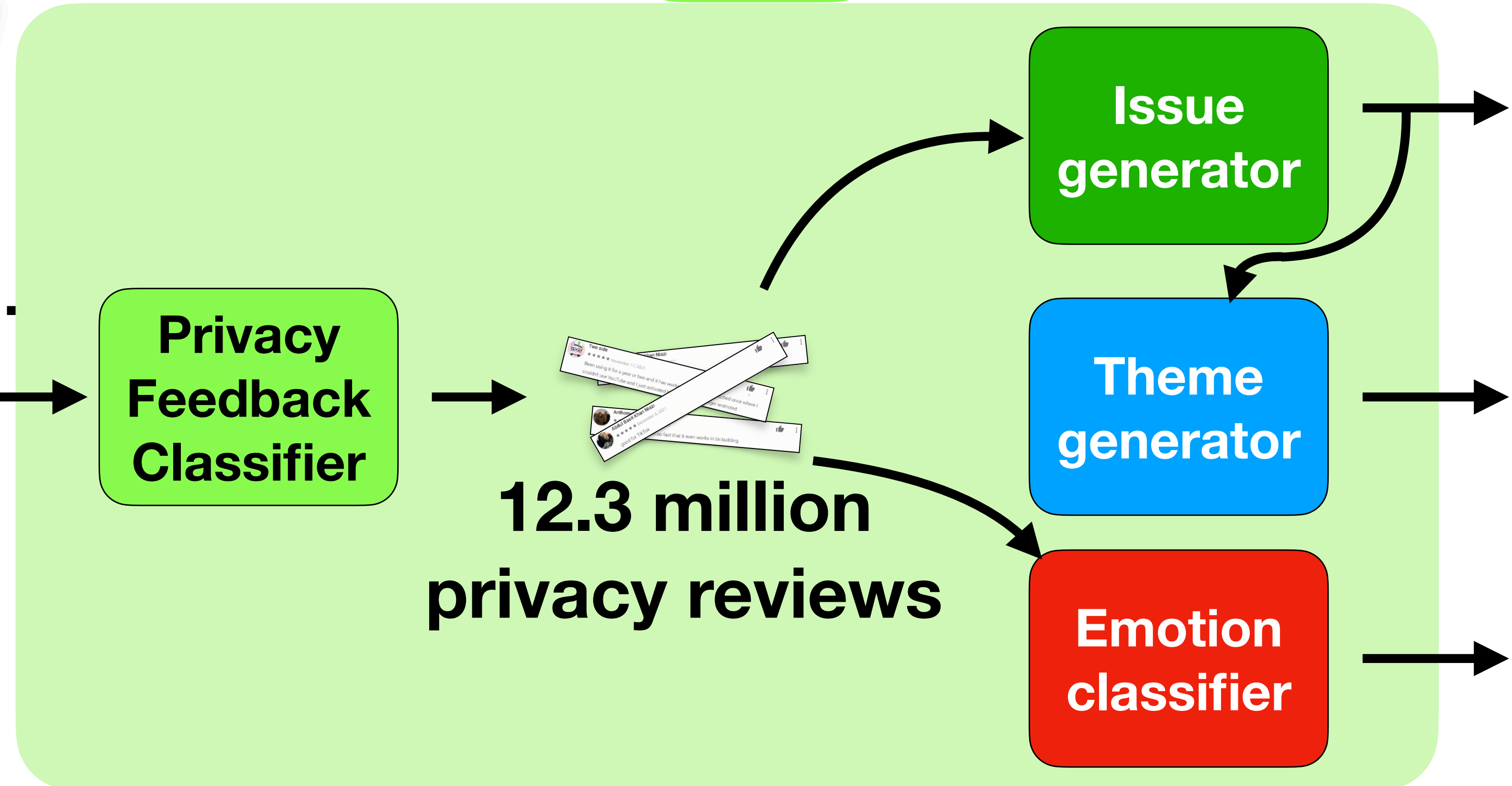


Our use: Analyze all Android app reviews!

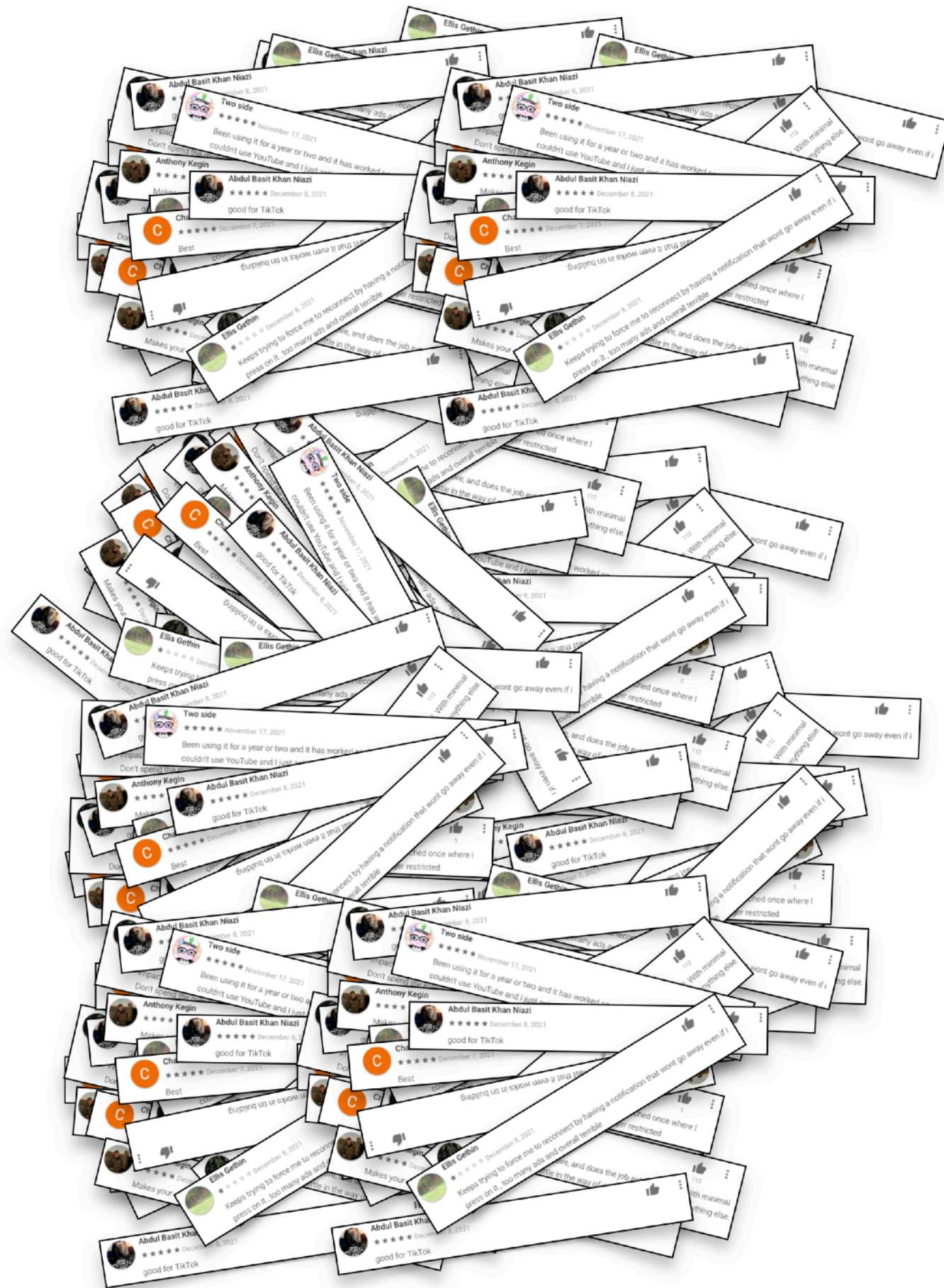
Hark!⁺



**~2 billion
public reviews**



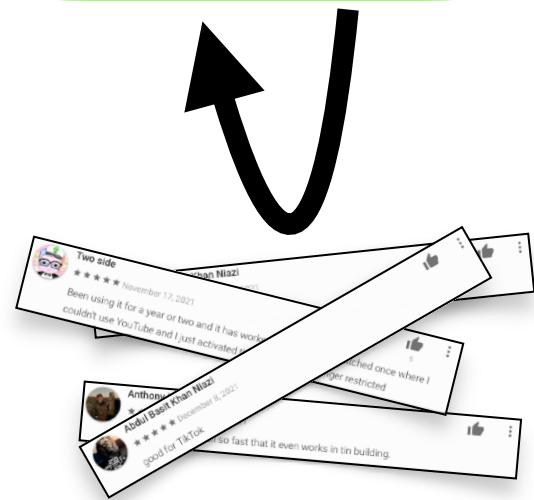
Our use: Analyze all Android app reviews!



**~2 billion
public reviews**

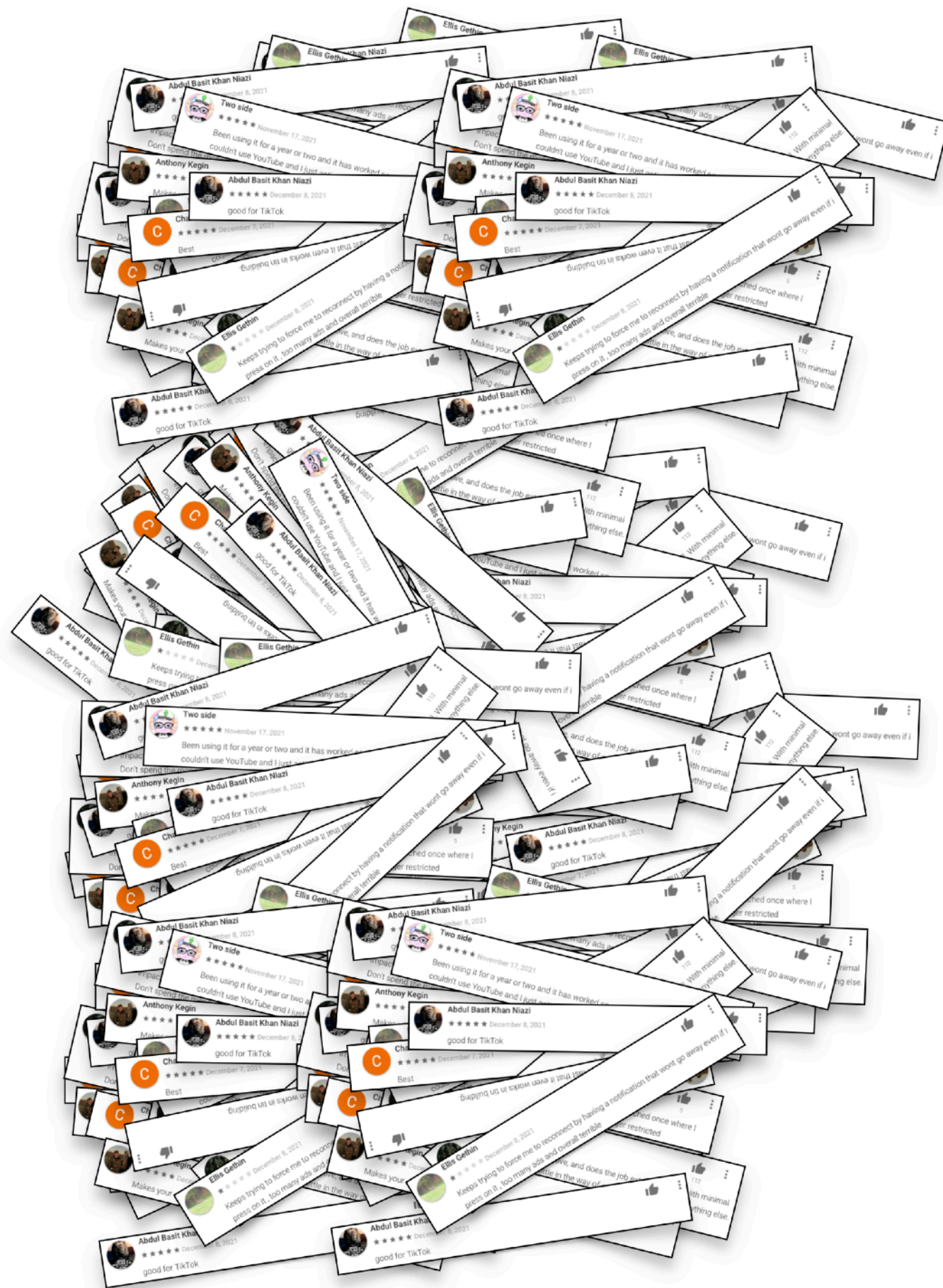


Hark!⁺



**12.3 million
privacy reviews**

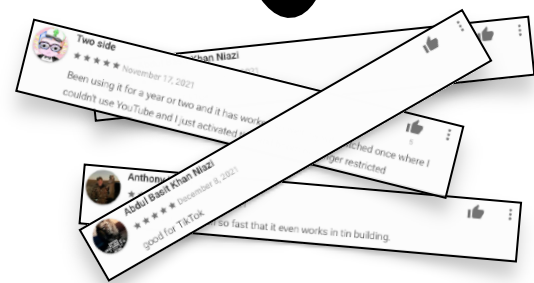
Our use: Analyze all Android app reviews!



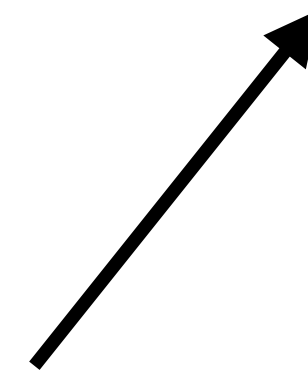
**~2 billion
public reviews**



Hark!⁺

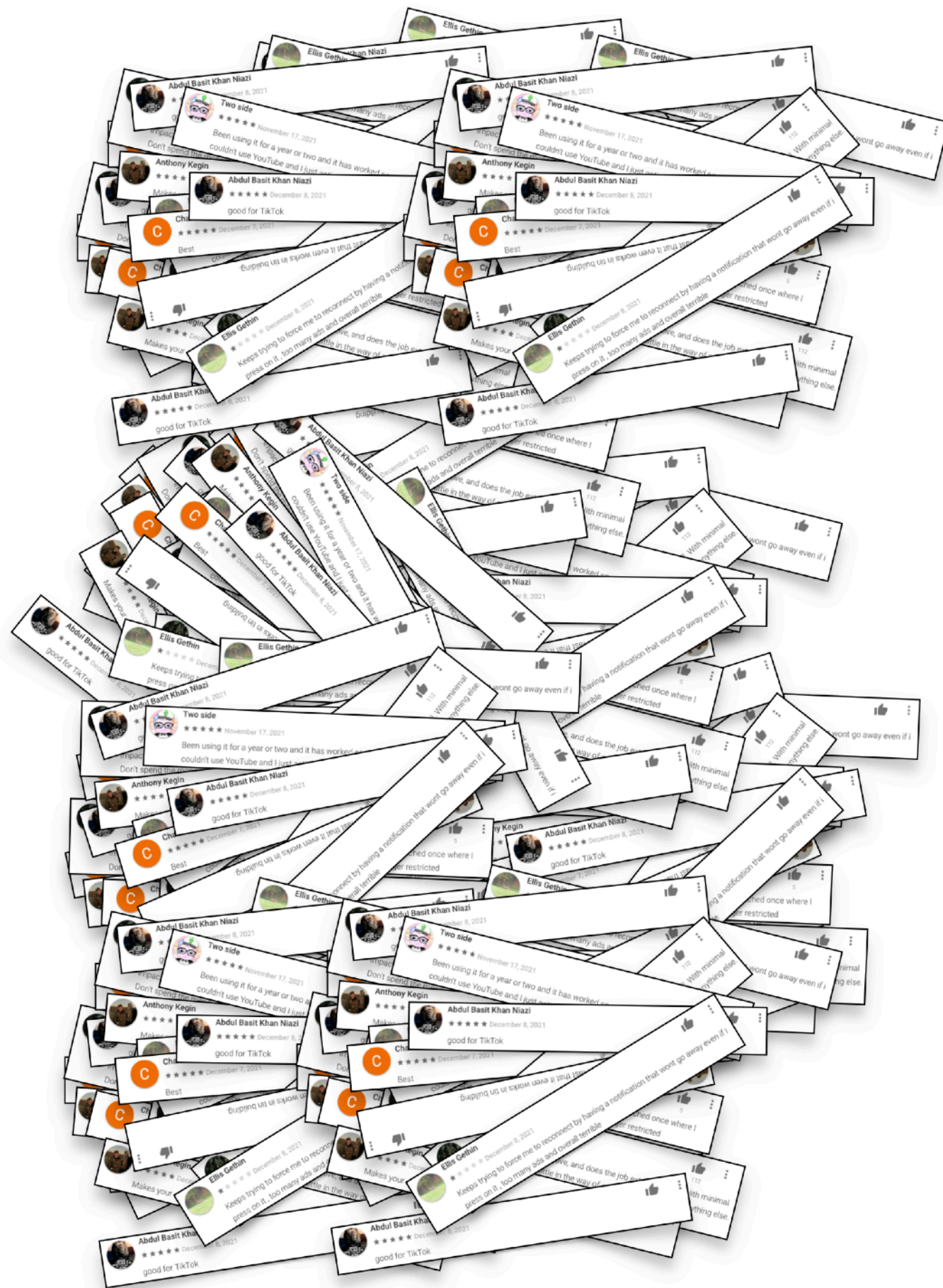


**12.3 million
privacy reviews**



**Granular
issues**

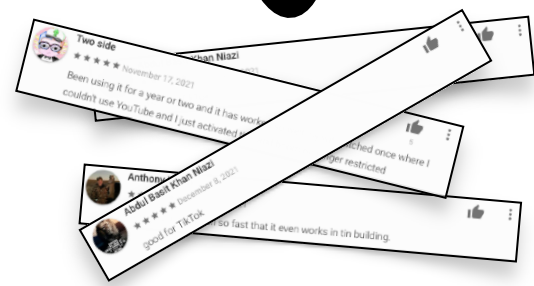
Our use: Analyze all Android app reviews!



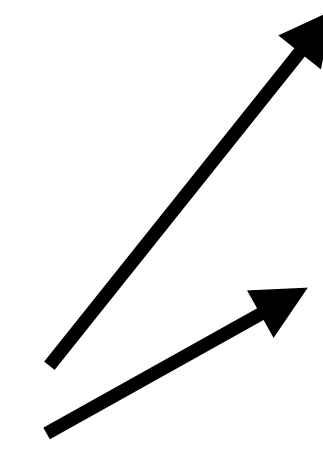
**~2 billion
public reviews**



Hark!⁺



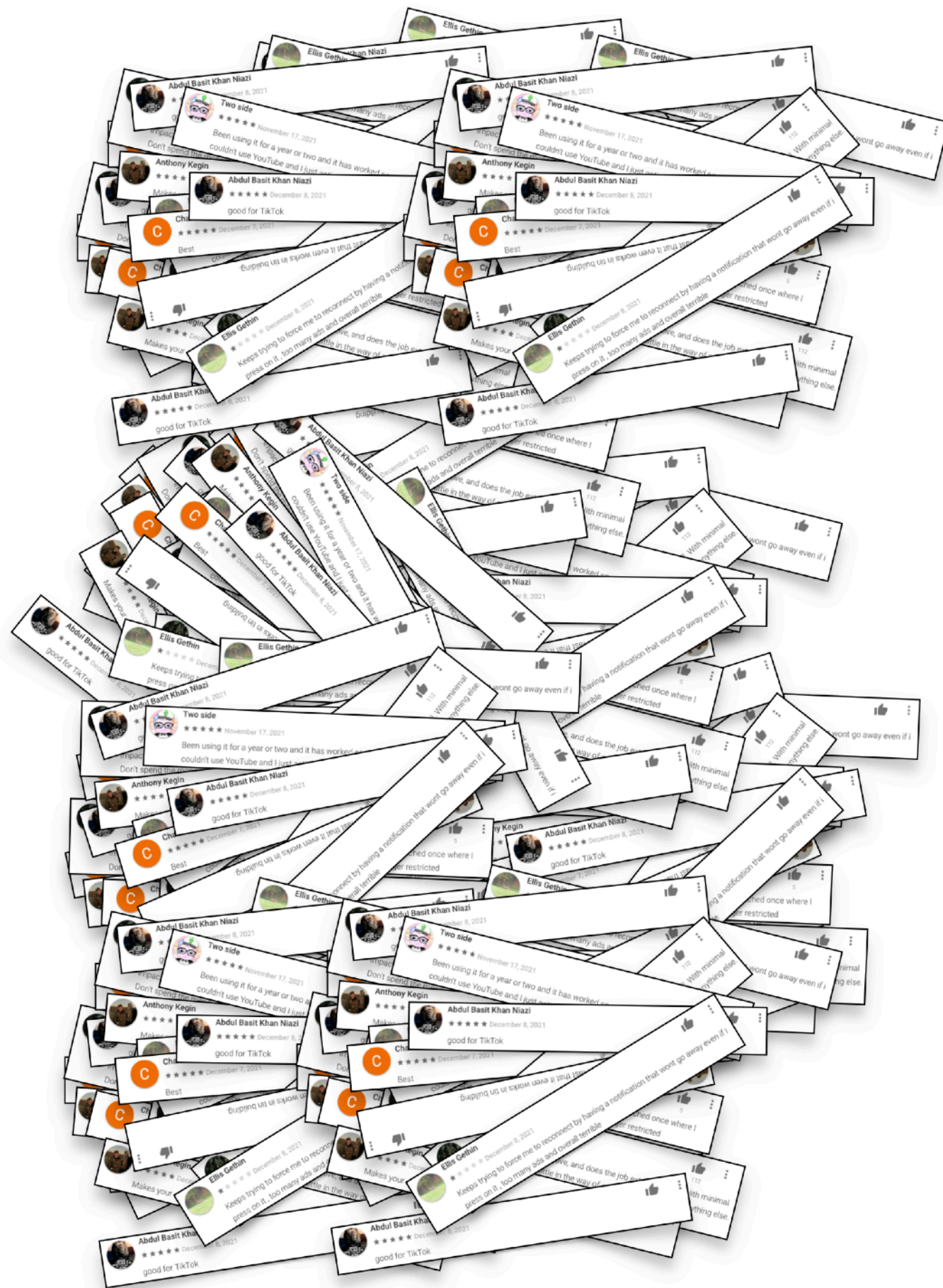
**12.3 million
privacy reviews**



**Granular
issues**

Themes

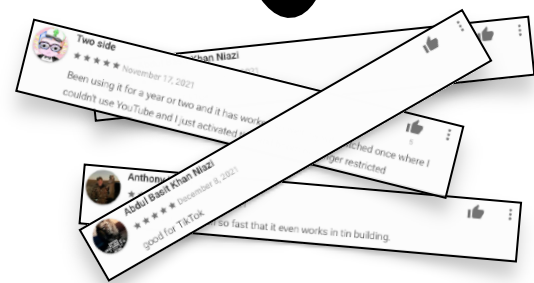
Our use: Analyze all Android app reviews!



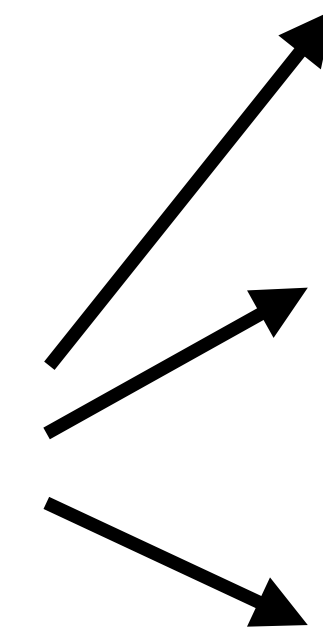
**~2 billion
public reviews**



Hark!⁺



**12.3 million
privacy reviews**

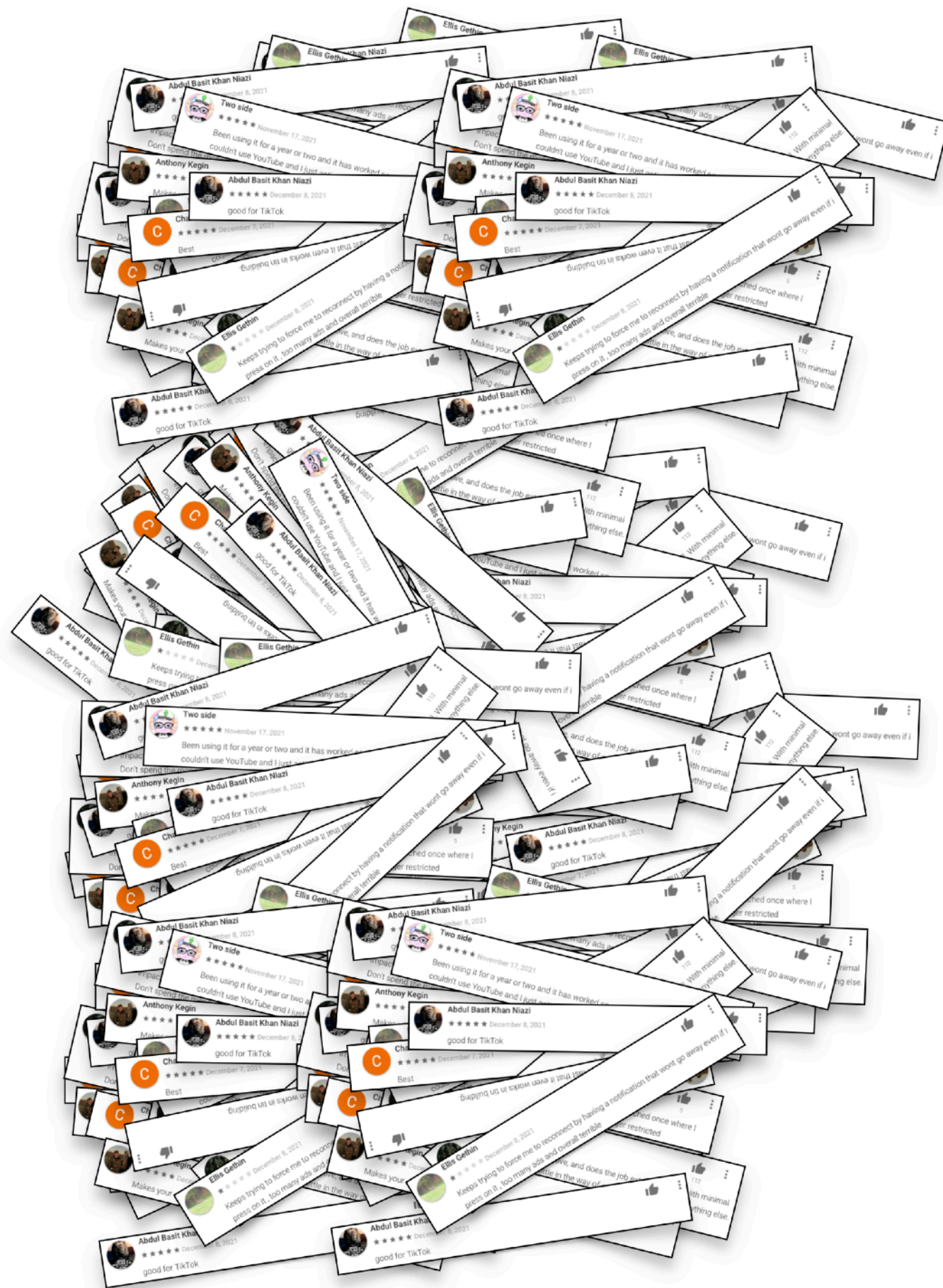


**Granular
issues**

Themes

Emotions

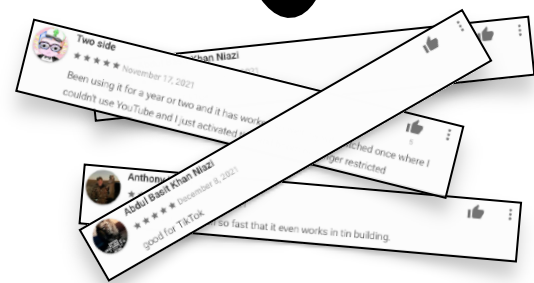
Our use: Analyze all Android app reviews!



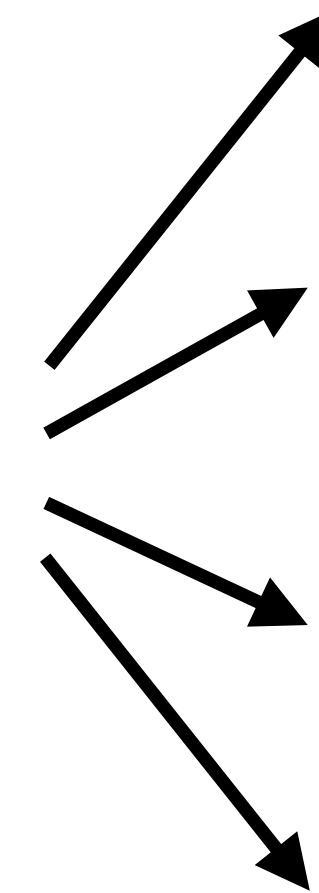
**~2 billion
public reviews**



Hark!⁺



**12.3 million
privacy reviews**



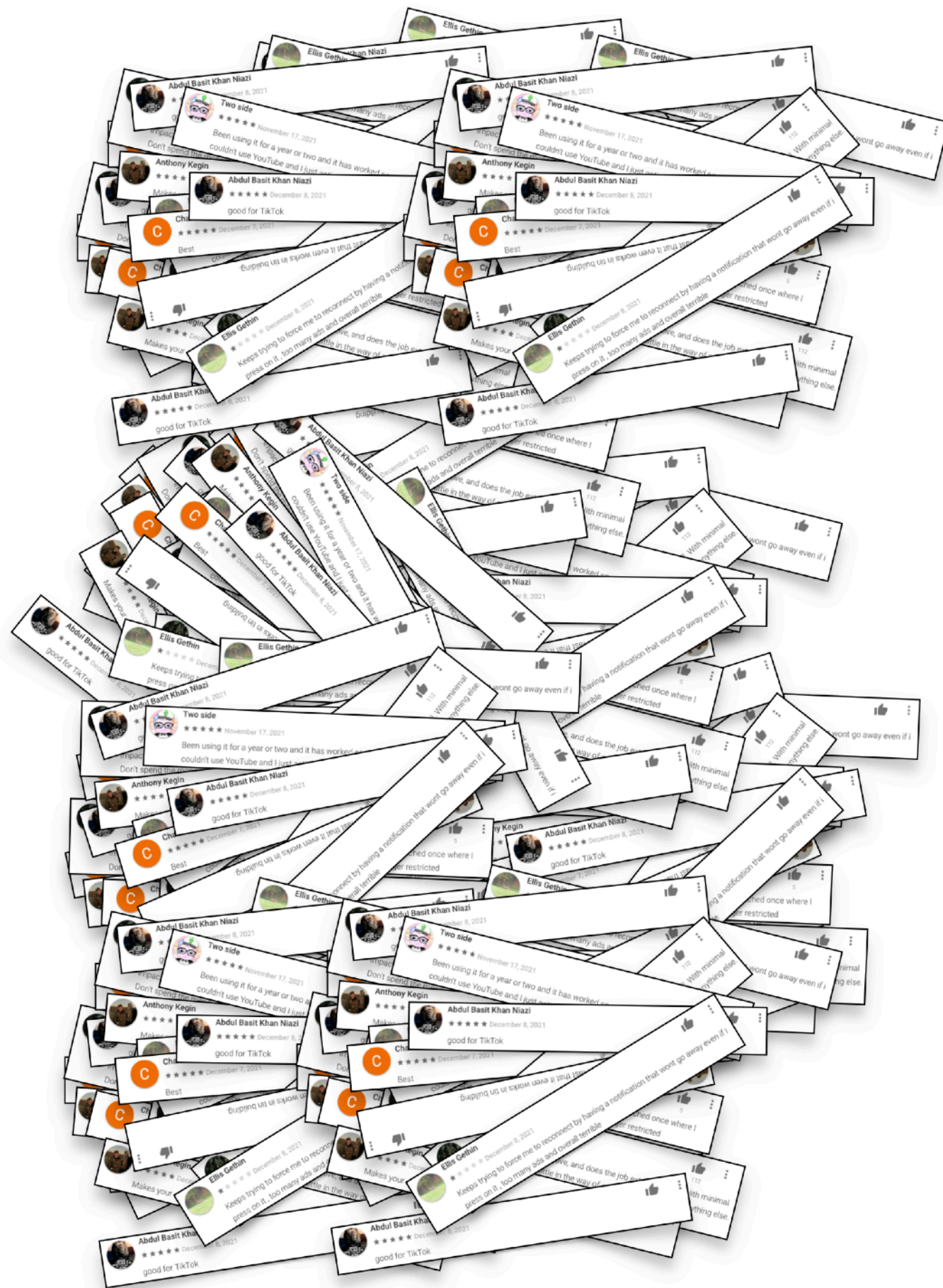
**Granular
issues**

Themes

Emotions

**Quality
quotes**

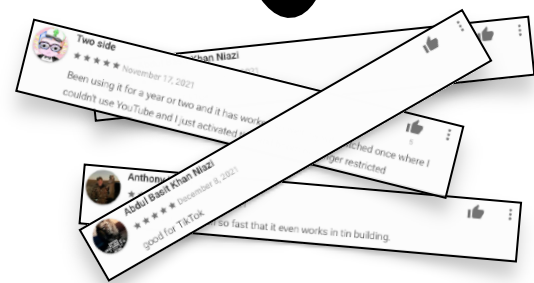
Our use: Analyze all Android app reviews!



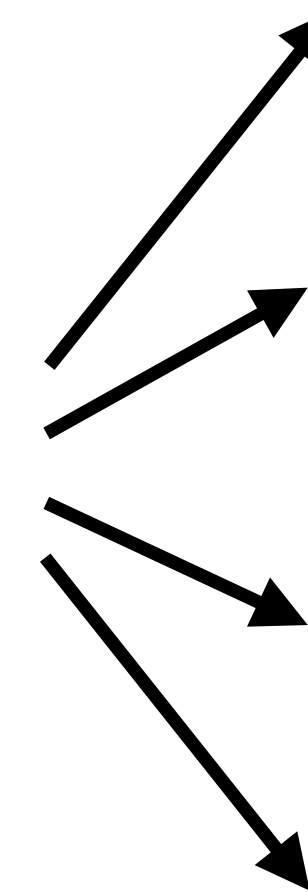
**~2 billion
public reviews**



Hark!⁺



**12.3 million
privacy reviews**

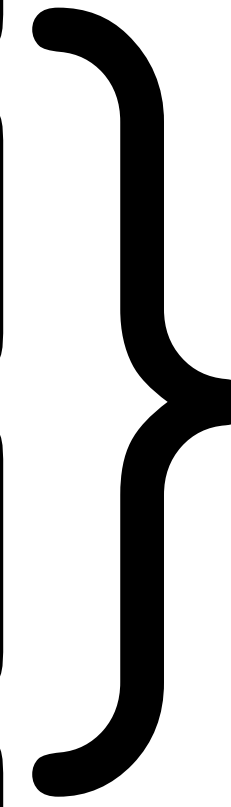


**Granular
issues**

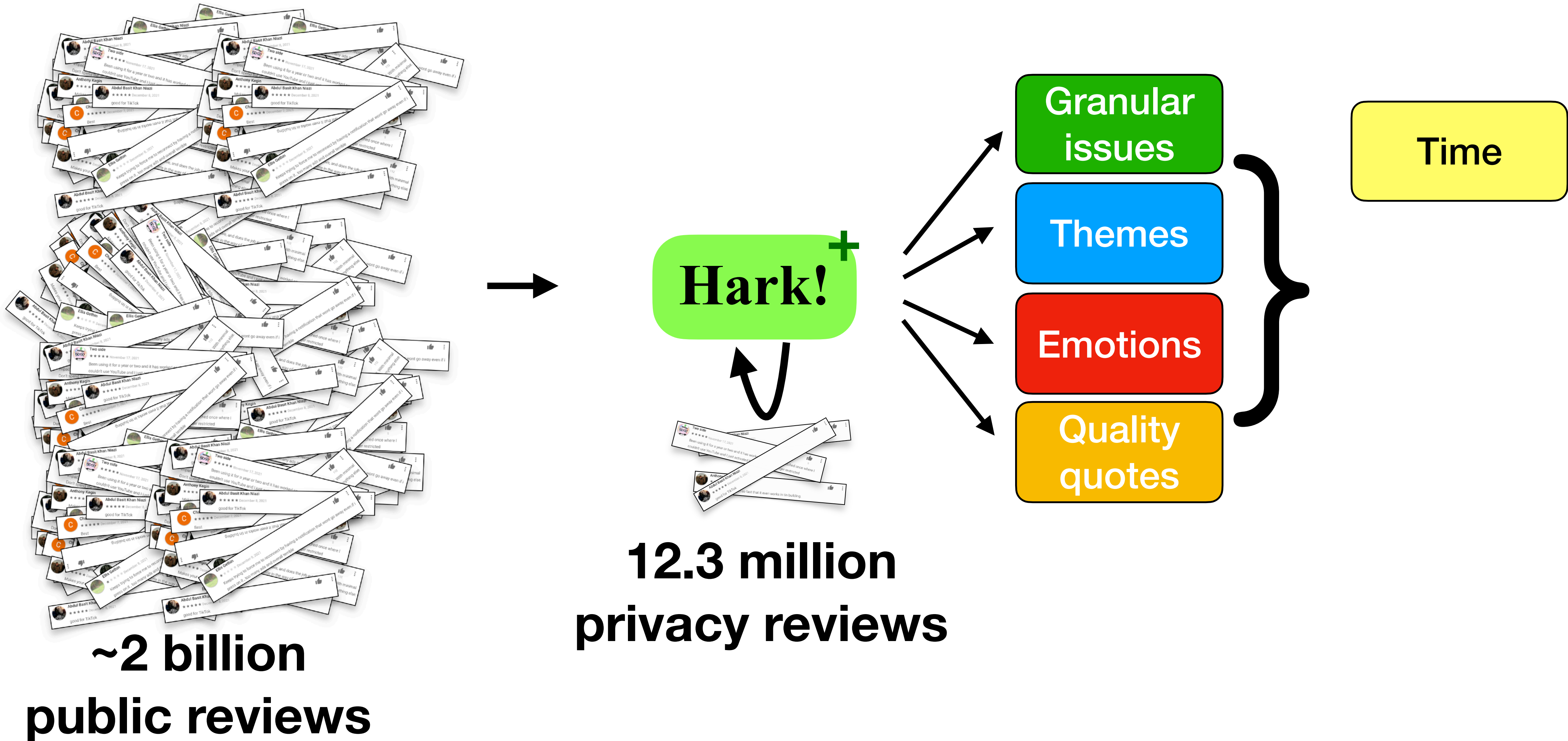
Themes

Emotions

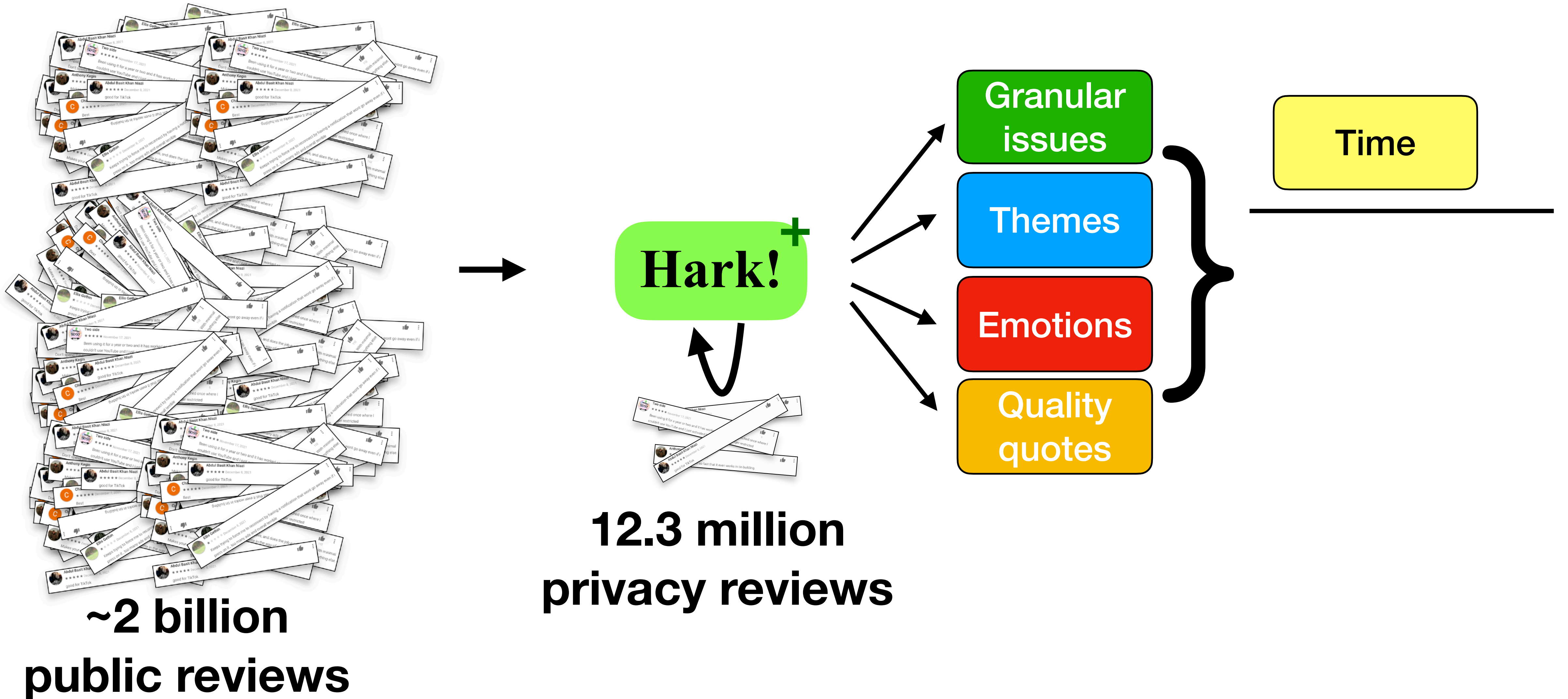
**Quality
quotes**



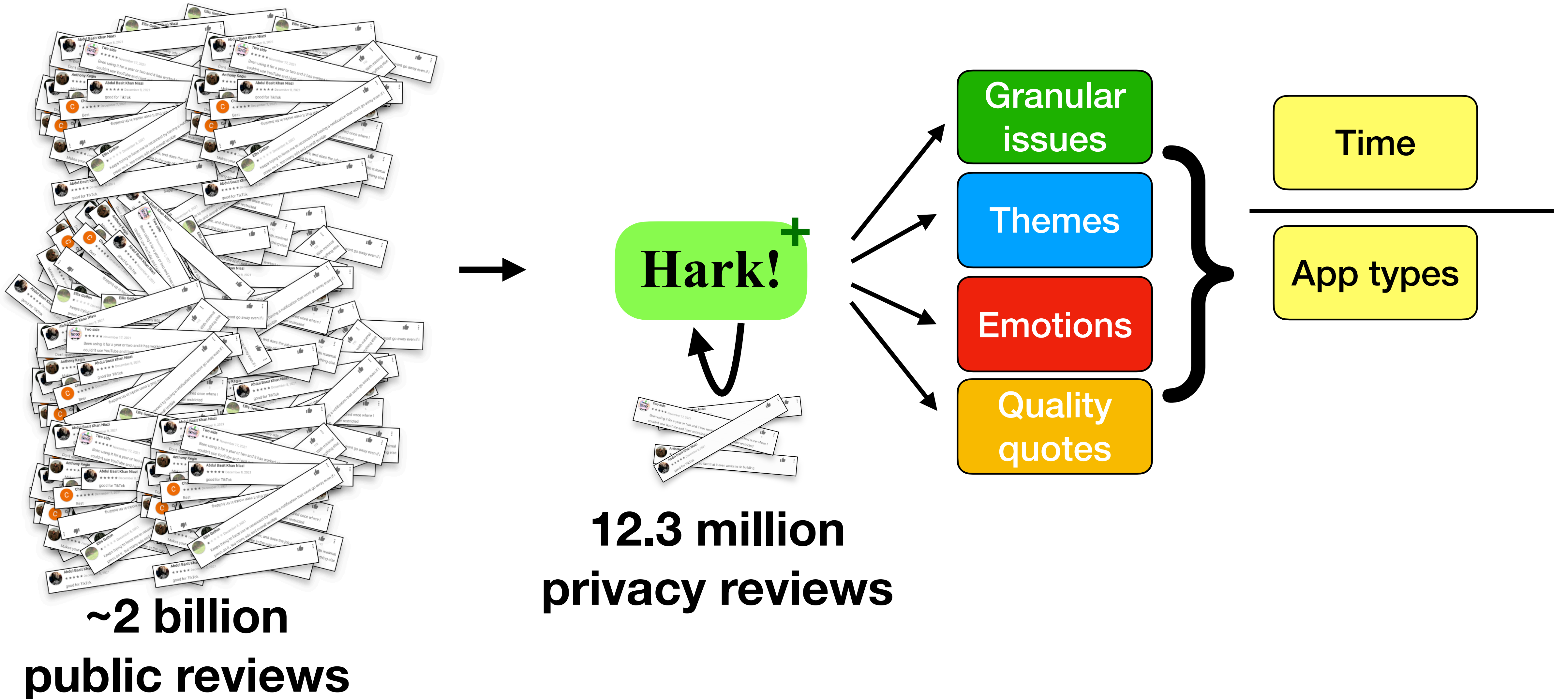
Our use: Analyze all Android app reviews!



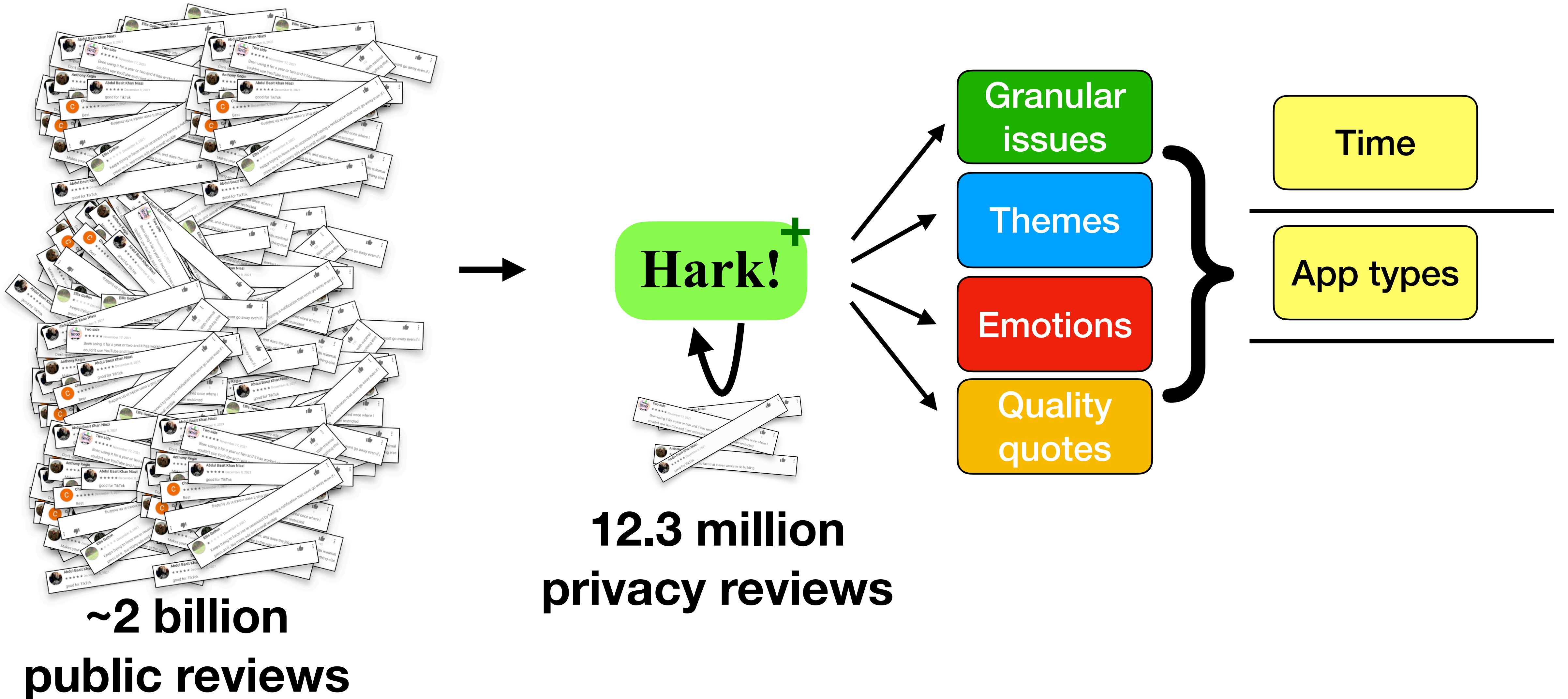
Our use: Analyze all Android app reviews!



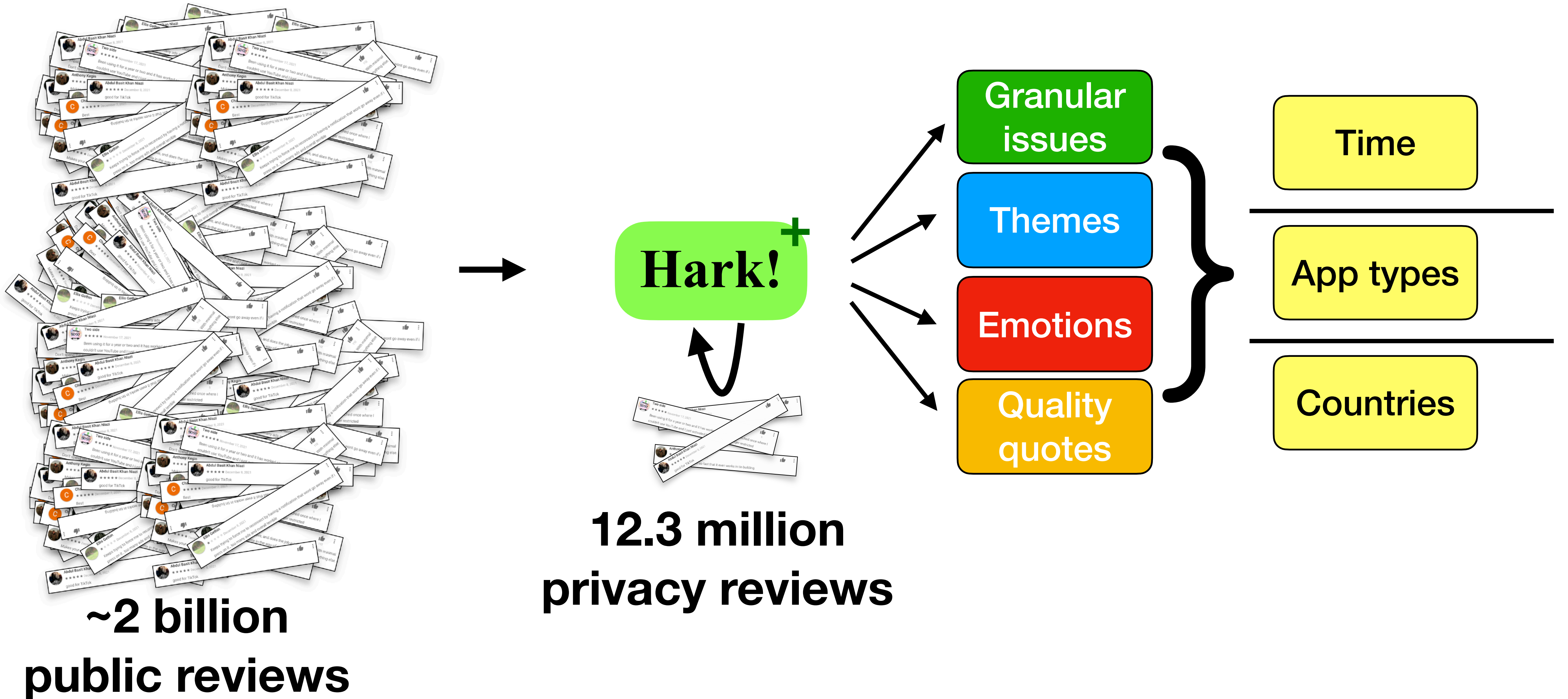
Our use: Analyze all Android app reviews!



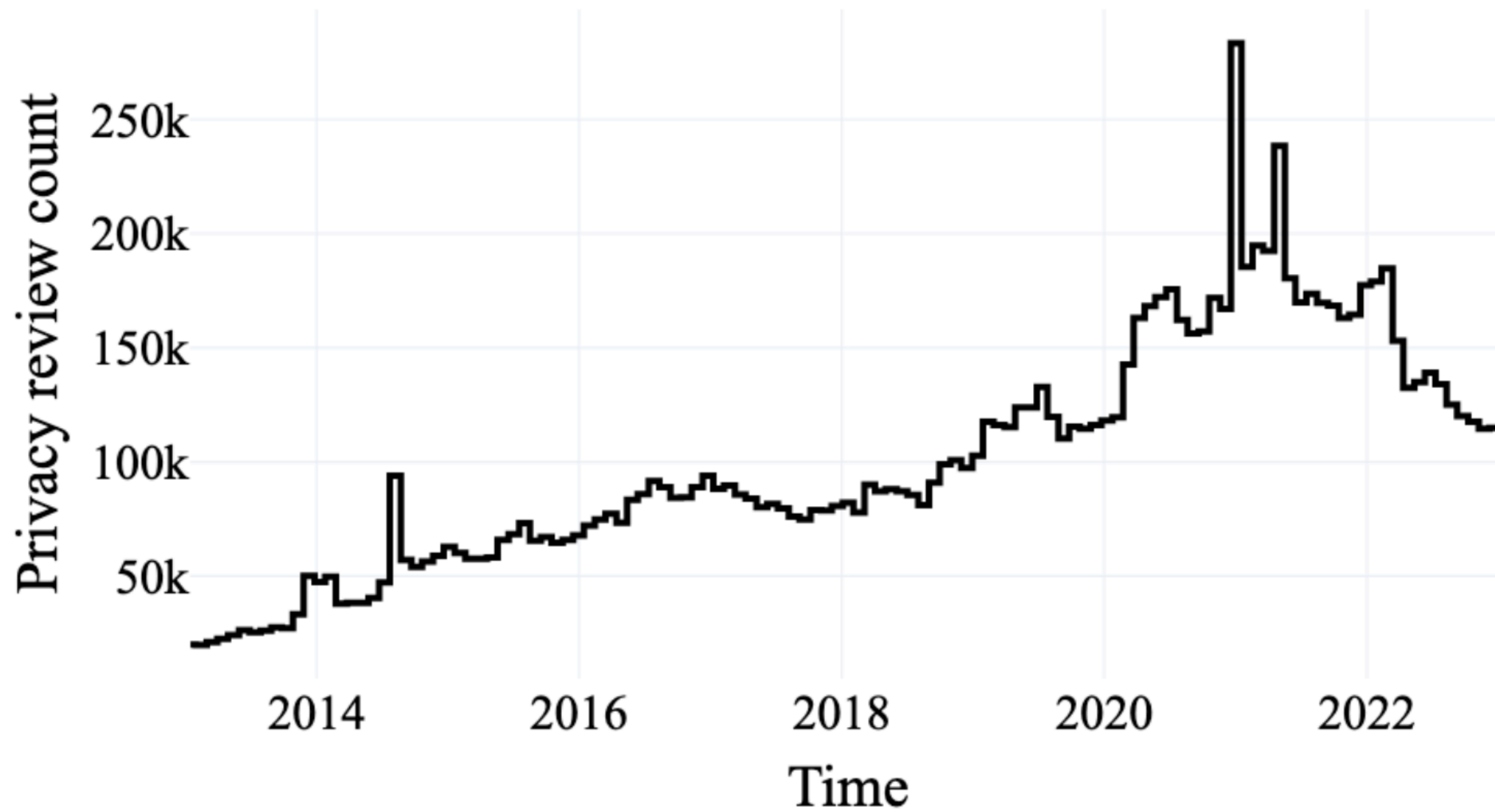
Our use: Analyze all Android app reviews!



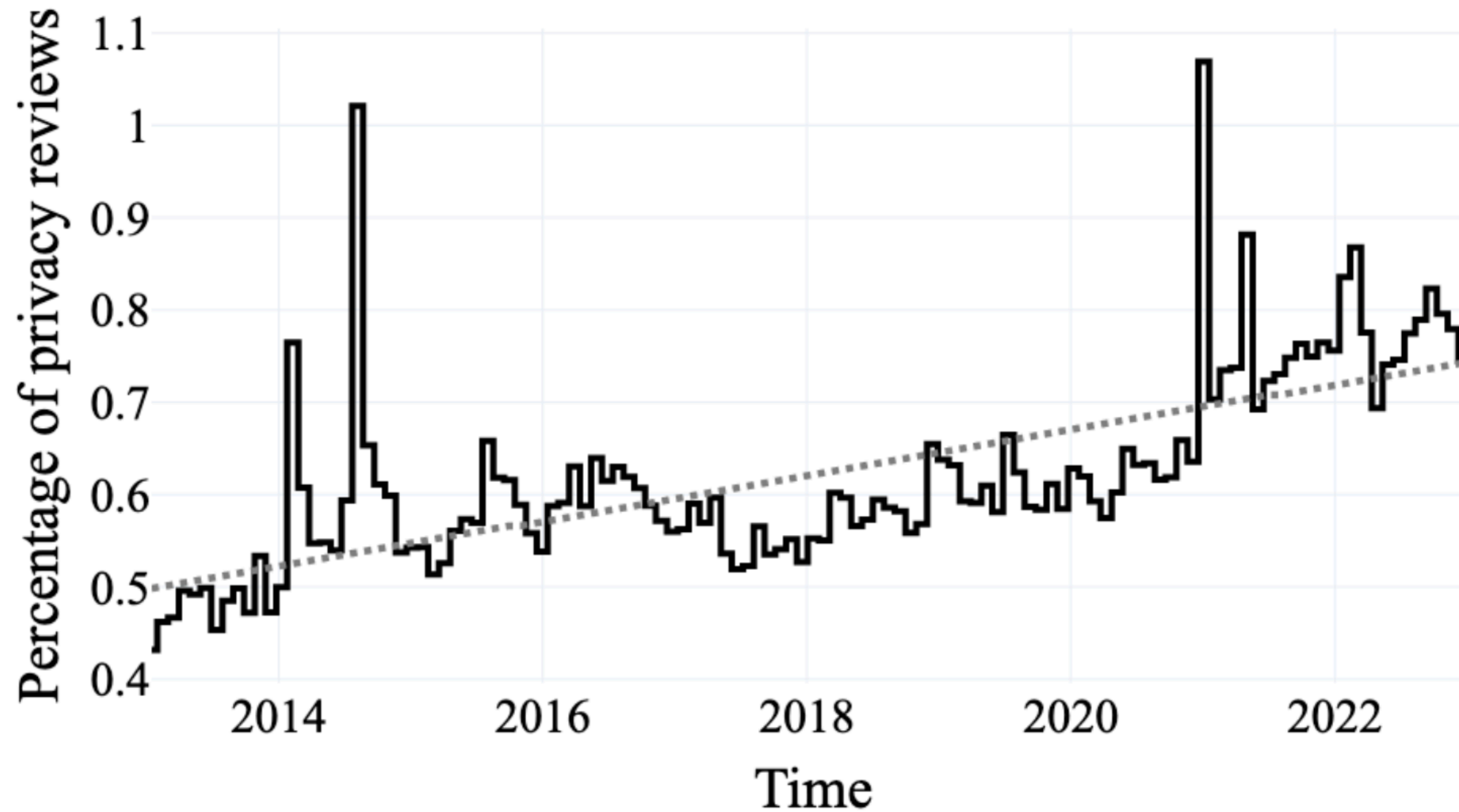
Our use: Analyze all Android app reviews!



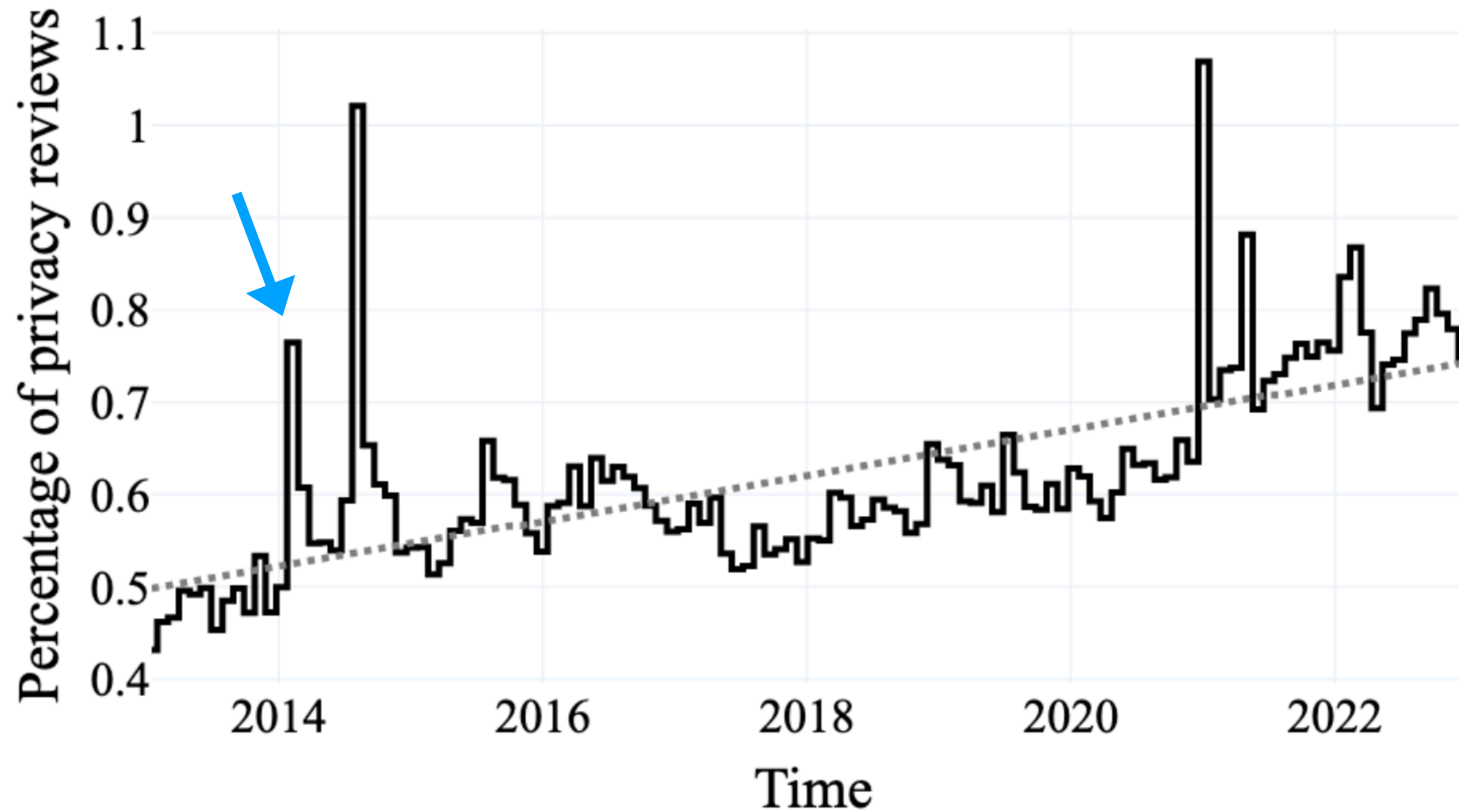
Privacy reviews go up ↑



Privacy reviews go up ↑



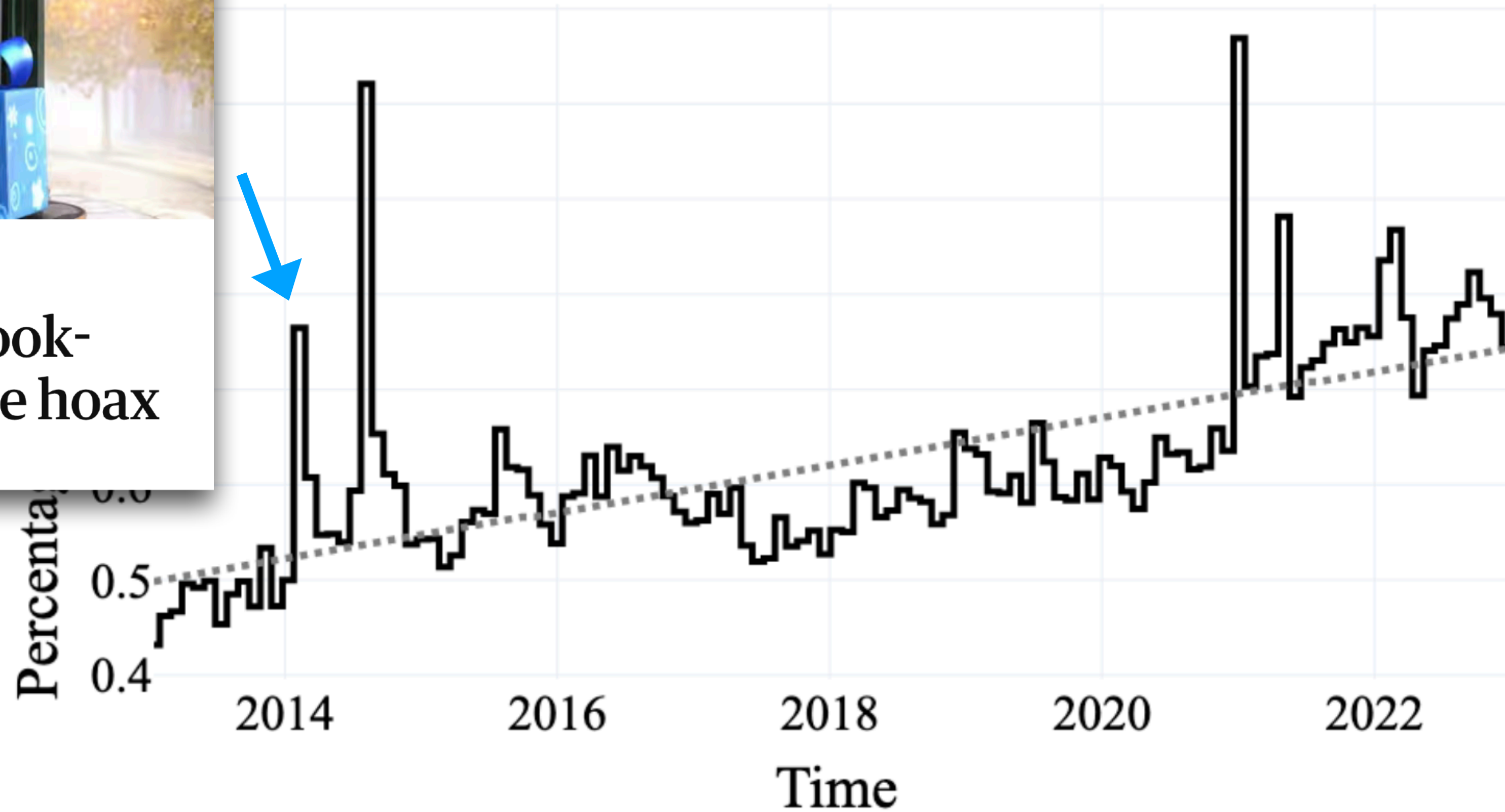
Privacy reviews go up ↑





Talking Angela developer: Facebook-fuelled paedophile hoax is 'ridiculous'

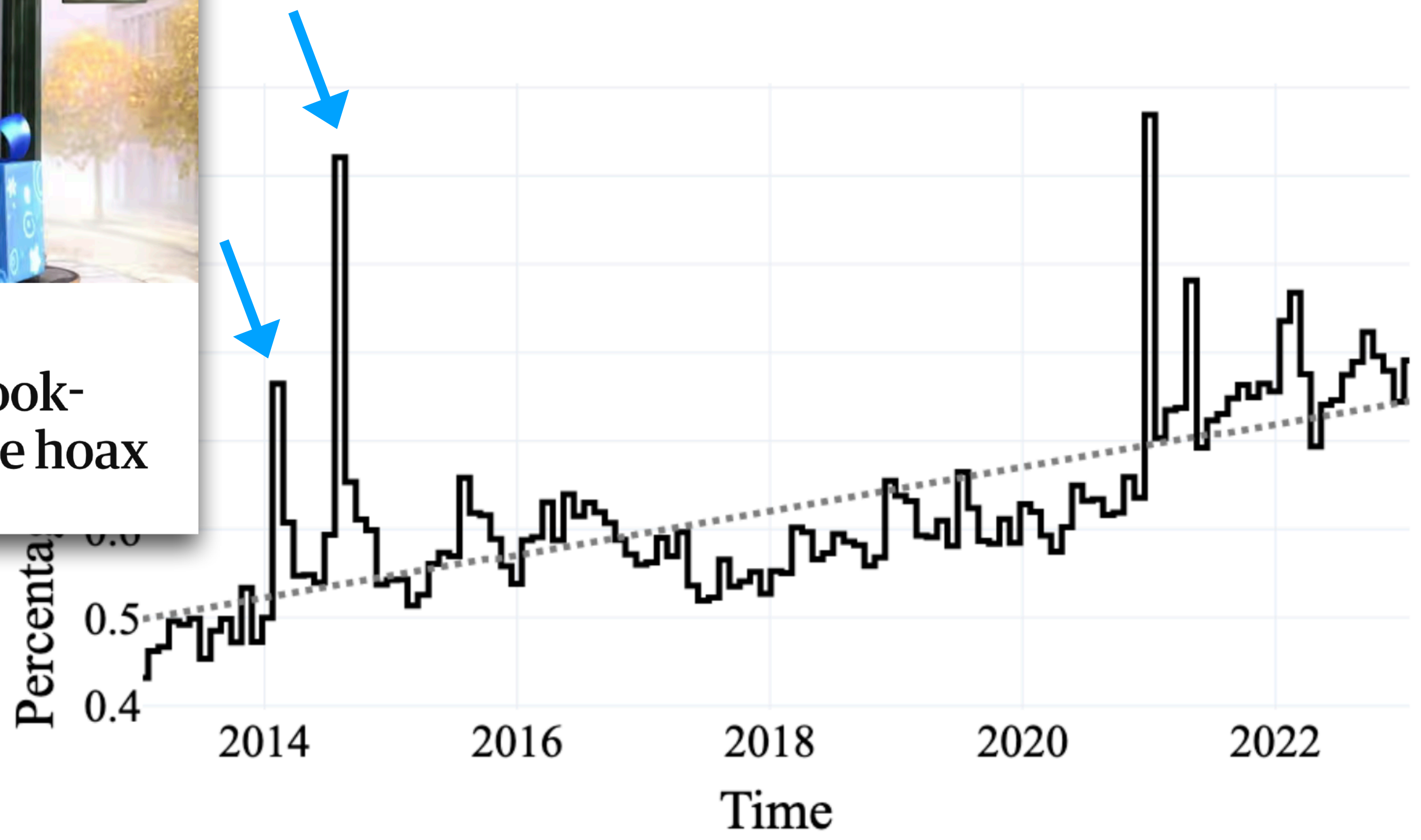
Privacy reviews go up ↑





Talking Angela developer: Facebook-fuelled paedophile hoax is 'ridiculous'

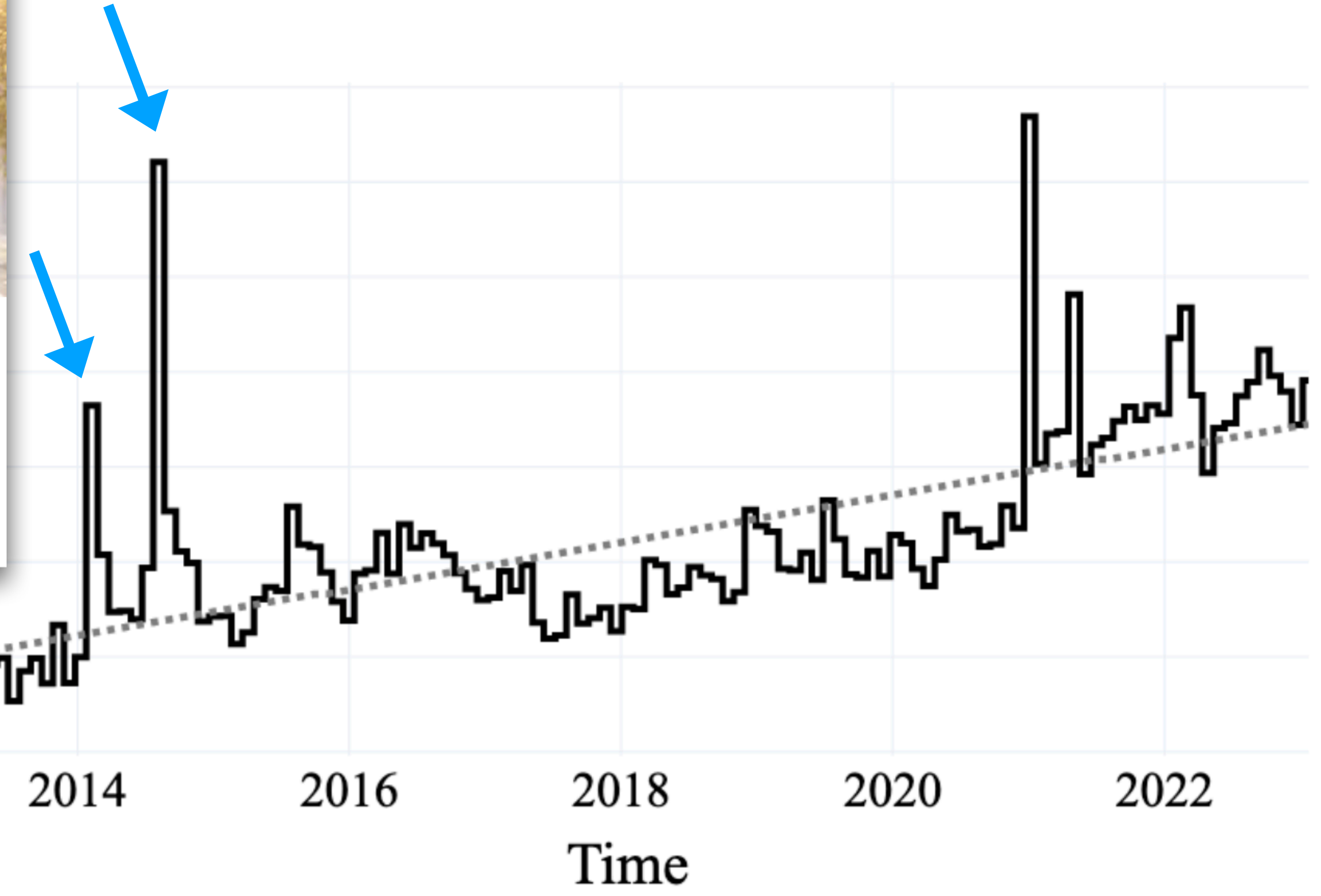
Privacy reviews go up ↑





Talking Angela developer: Facebook-fuelled paedophile hoax is 'ridiculous'

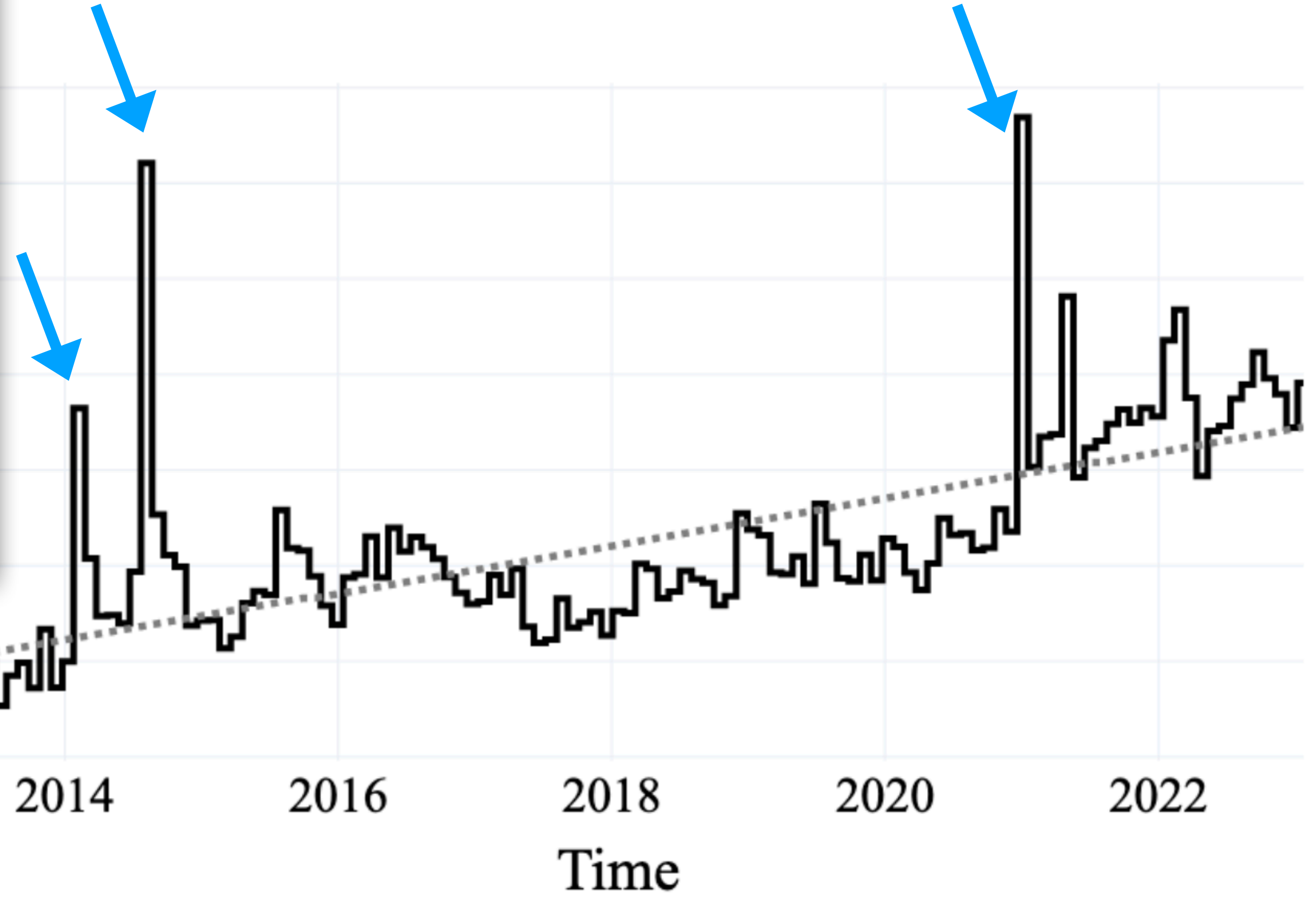
Privacy reviews go up ↑





Talking Angela developer: Facebook-fuelled paedophile hoax is 'ridiculous'

Privacy reviews go up ↑



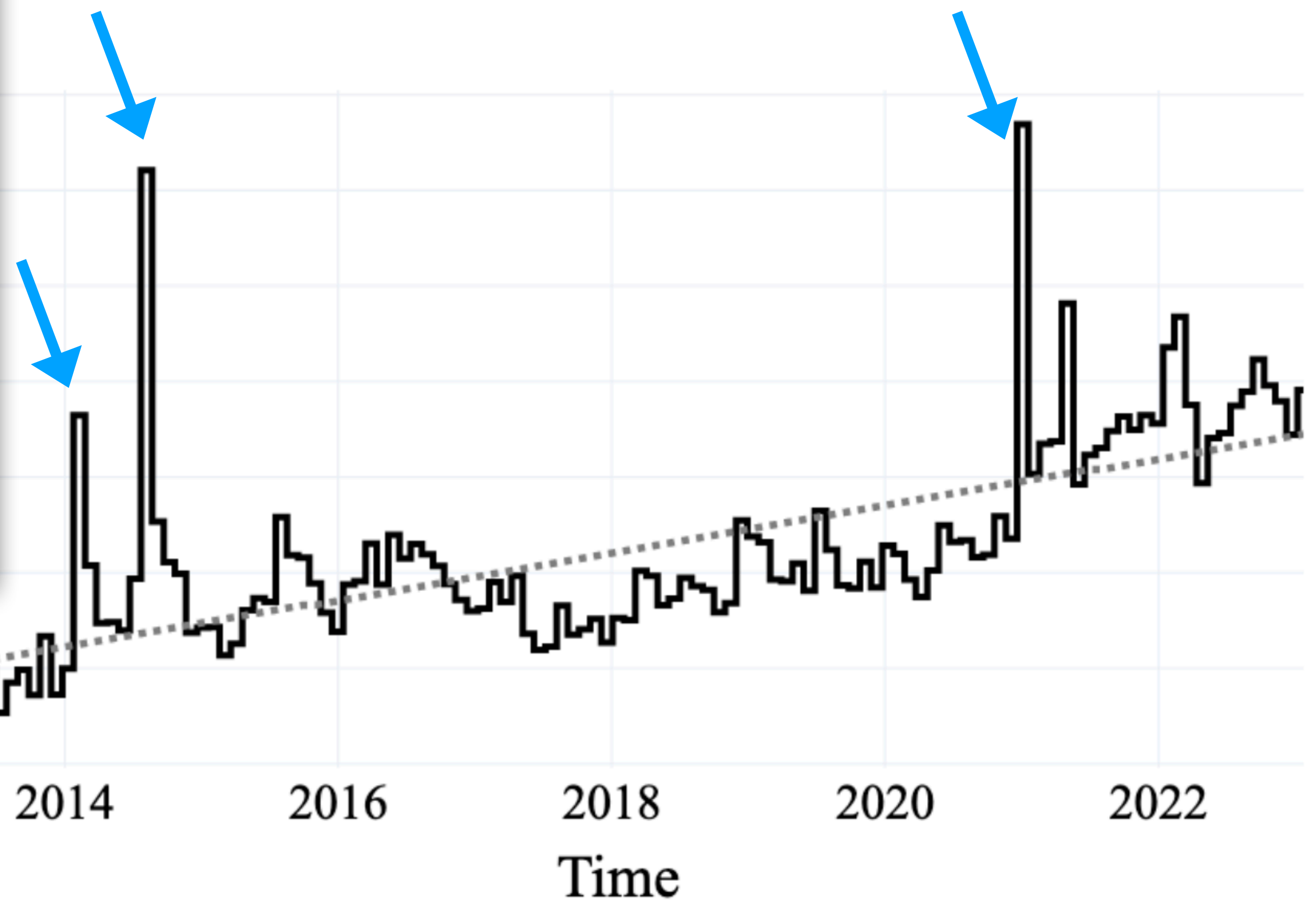
The Guardian

Support us



Talking Angela developer: Facebook-fuelled paedophile hoax is 'ridiculous'

Privacy reviews go up ↑



The Guardian

Support us



Talking Angela developer: Facebook-fuelled paedophile hoax is 'ridiculous'

Privacy reviews go up ↑



The Guardian

Support us



Talking Angela developer: Facebook-fuelled paedophile hoax is 'ridiculous'

Privacy reviews go up ↑



Q: Consistent increase across

Q: Consistent increase across
themes,

Q: Consistent increase across

themes,

countries,

Q: Consistent increase across

themes, countries, app types?

Q: Consistent increase across

themes, countries, app types?

NO!

Q: Consistent increase across

themes, countries, app types?

NO!

NO!

Q: Consistent increase across

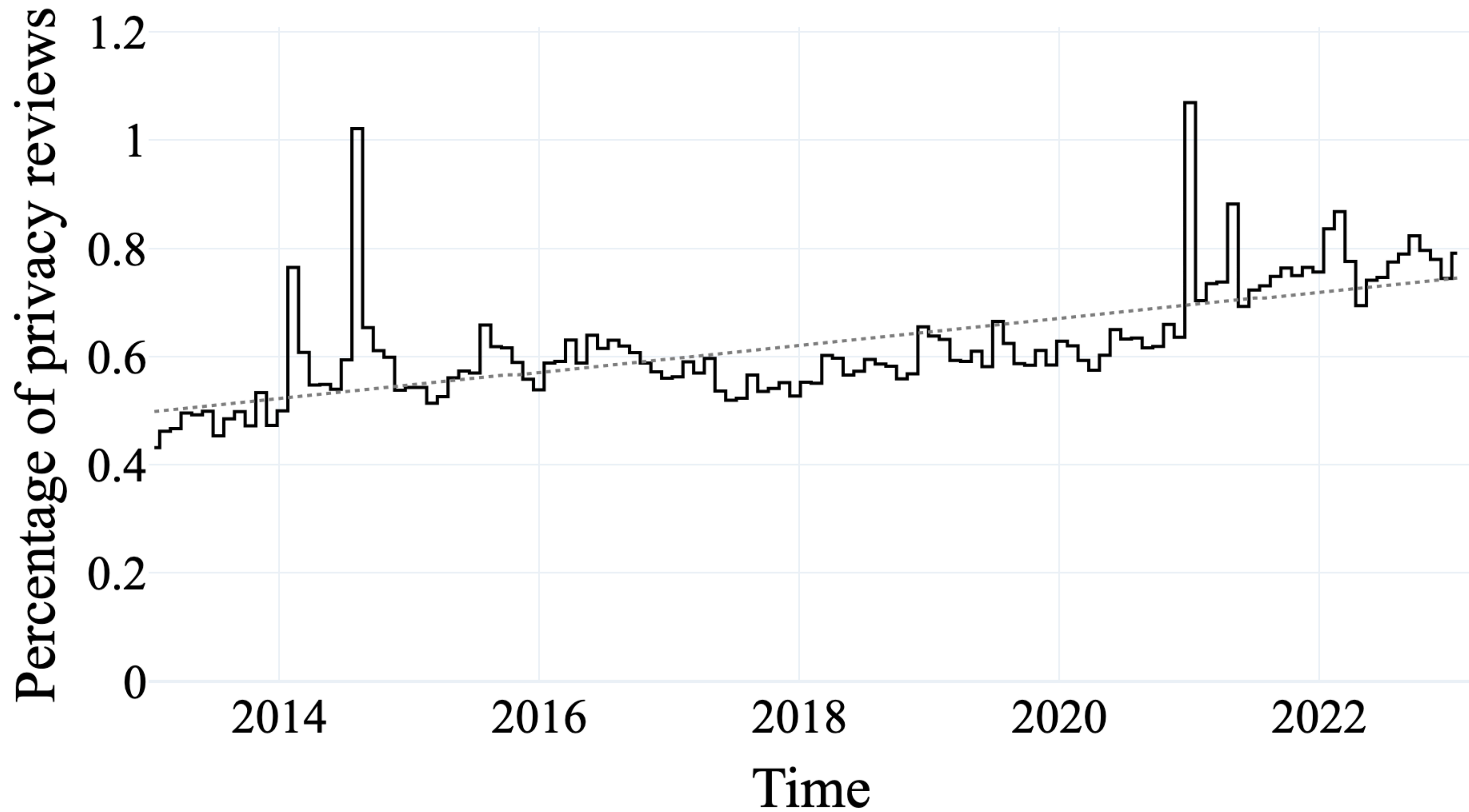
themes, countries, app types?

NO!

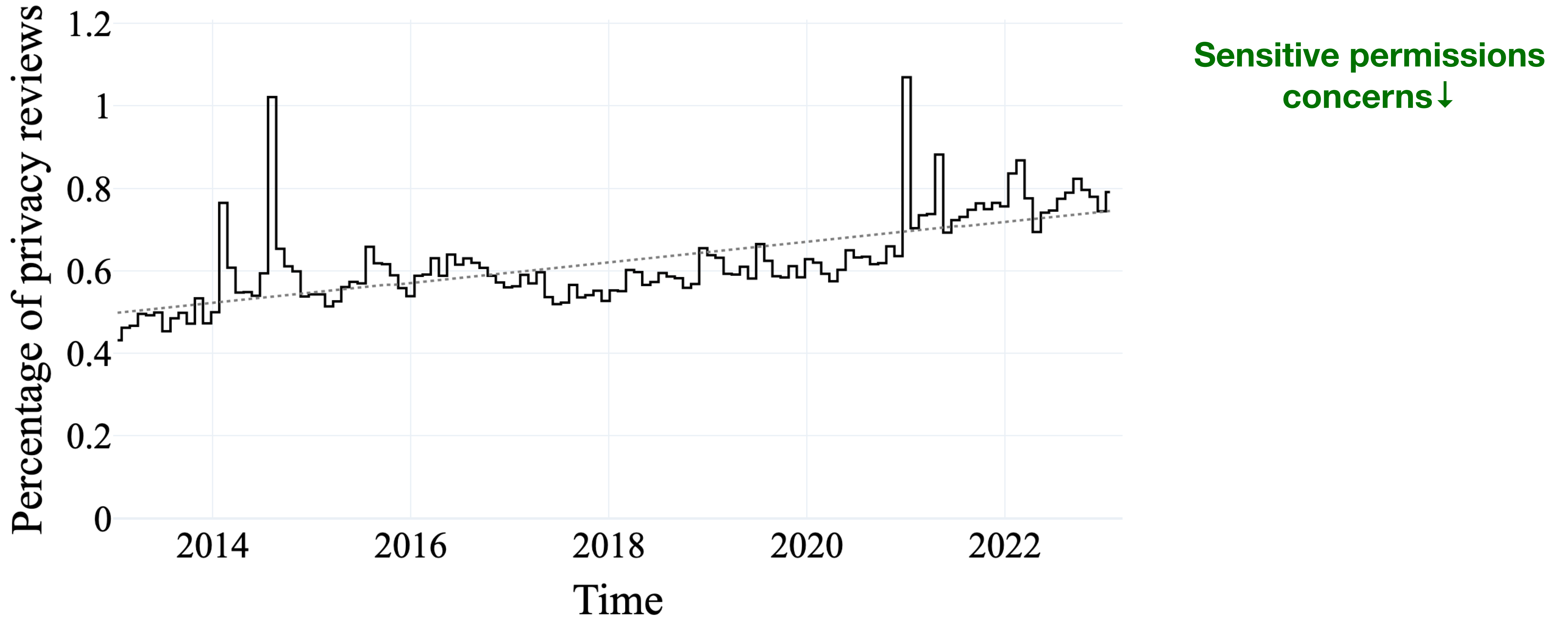
NO!

NO!

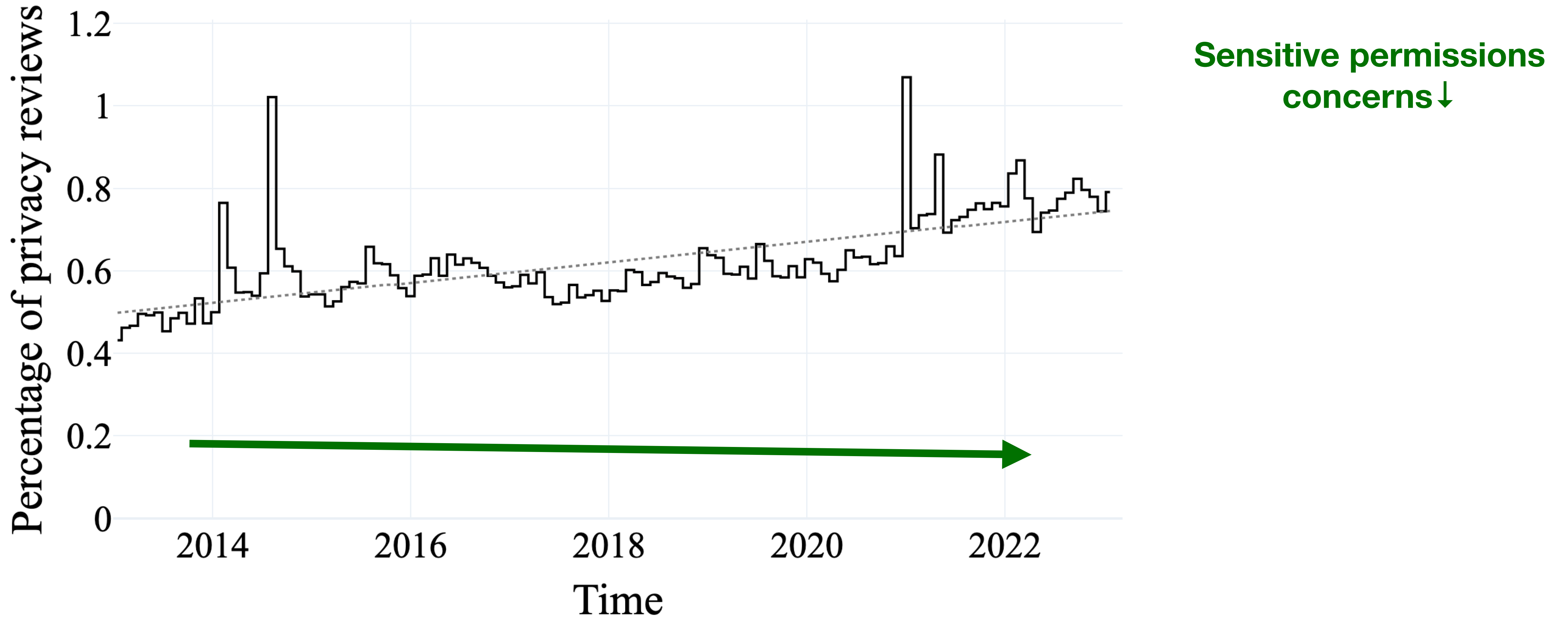
Themes change over time



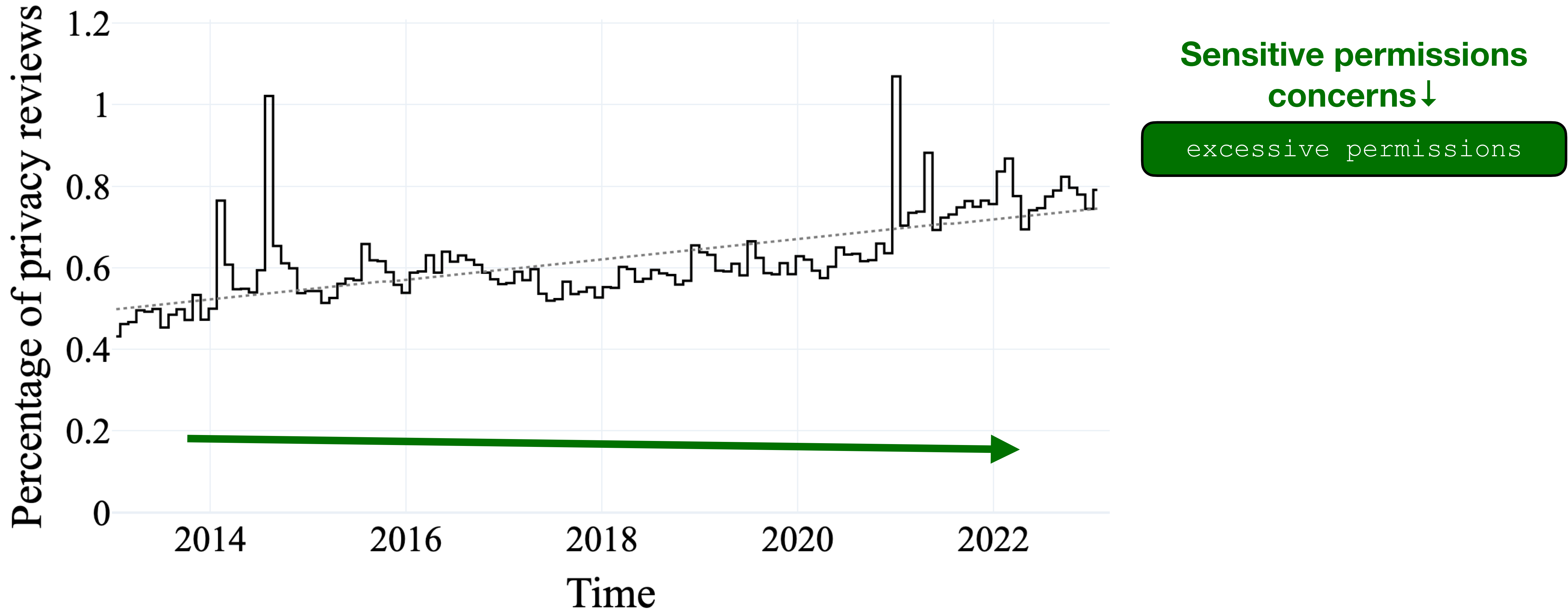
Themes change over time



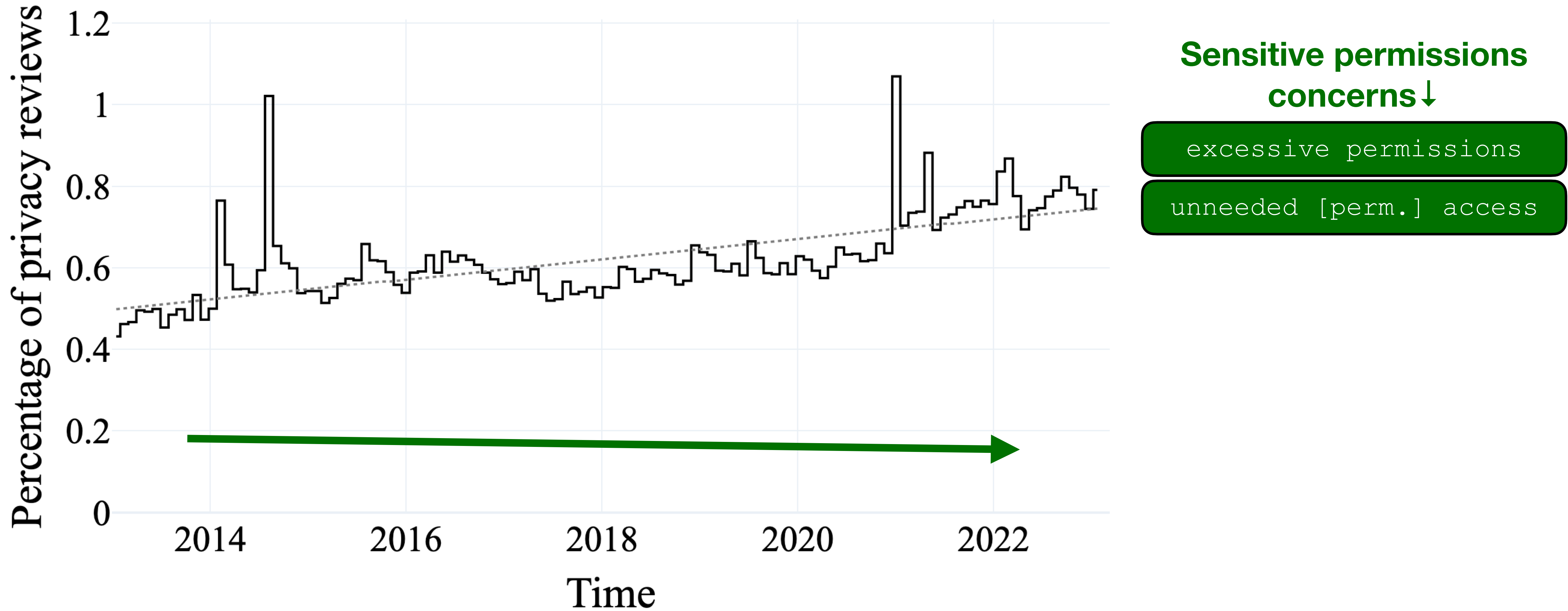
Themes change over time



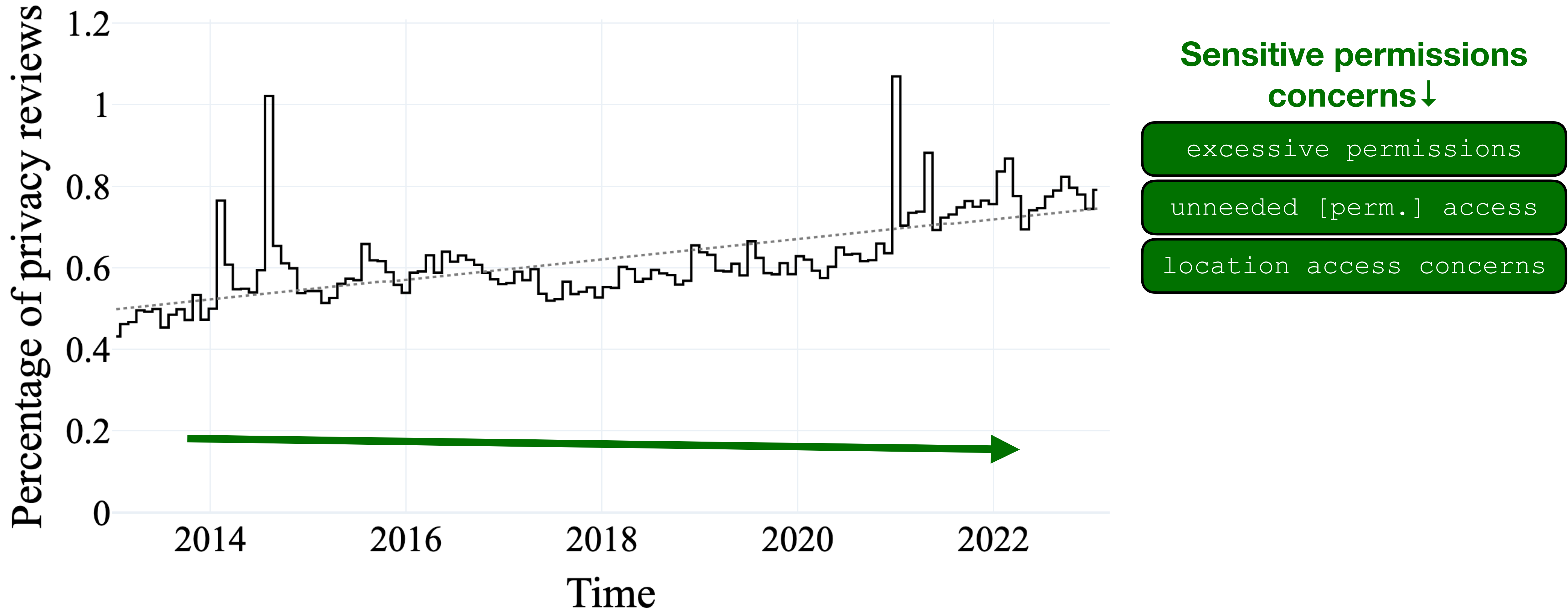
Themes change over time



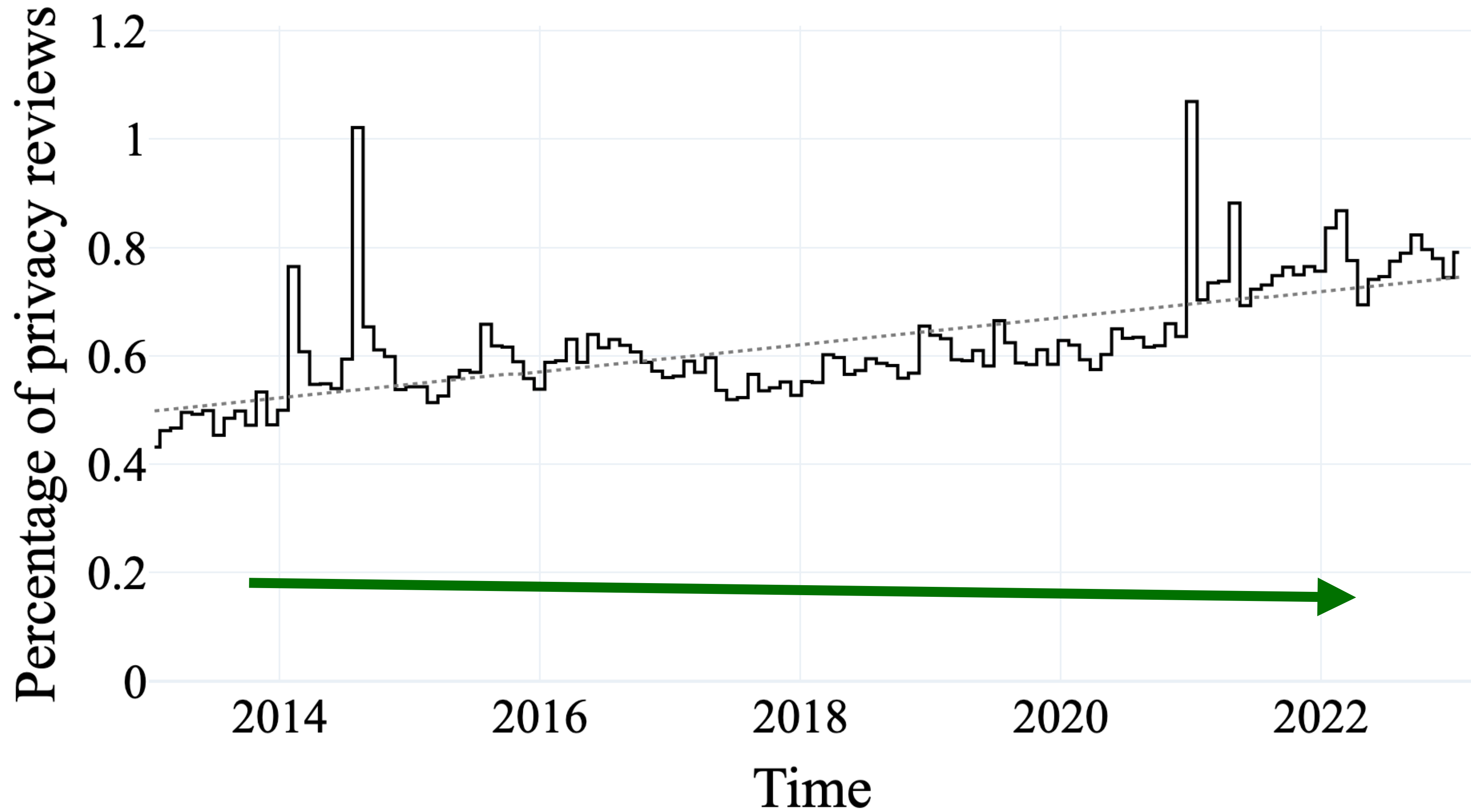
Themes change over time



Themes change over time



Themes change over time



Sensitive permissions concerns ↓

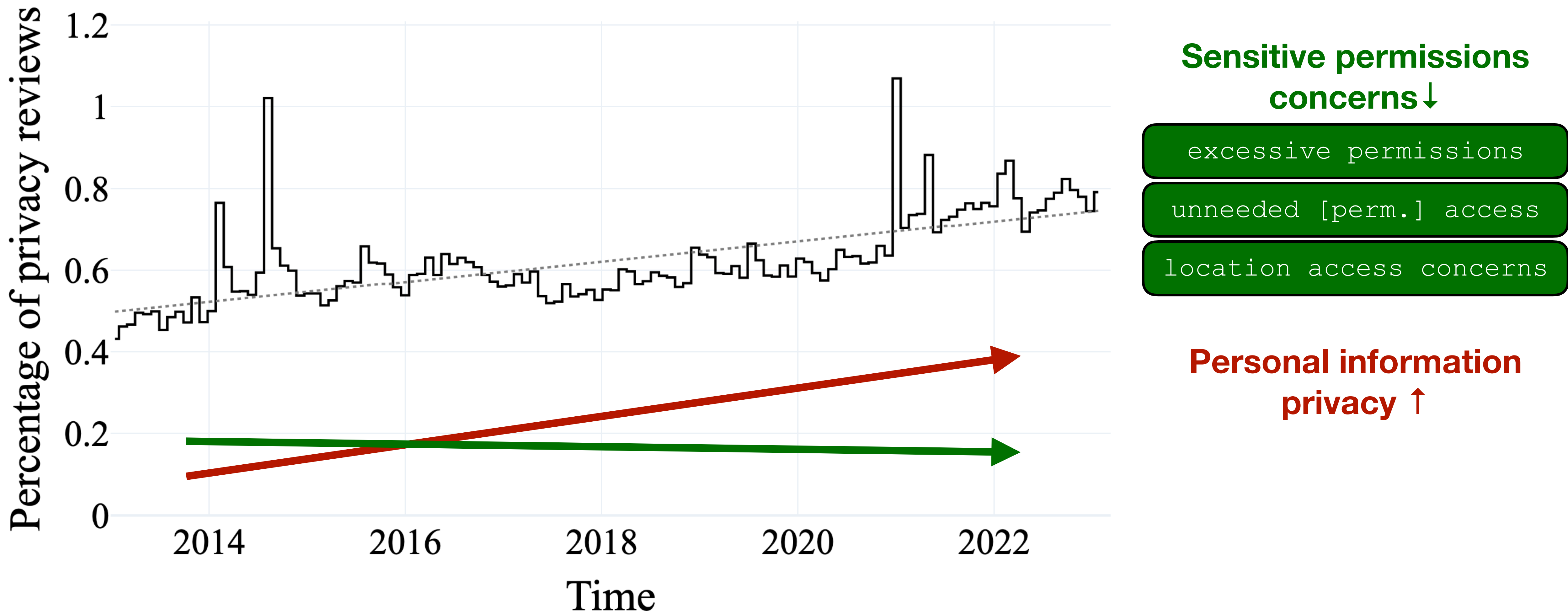
excessive permissions

unnneeded [perm.] access

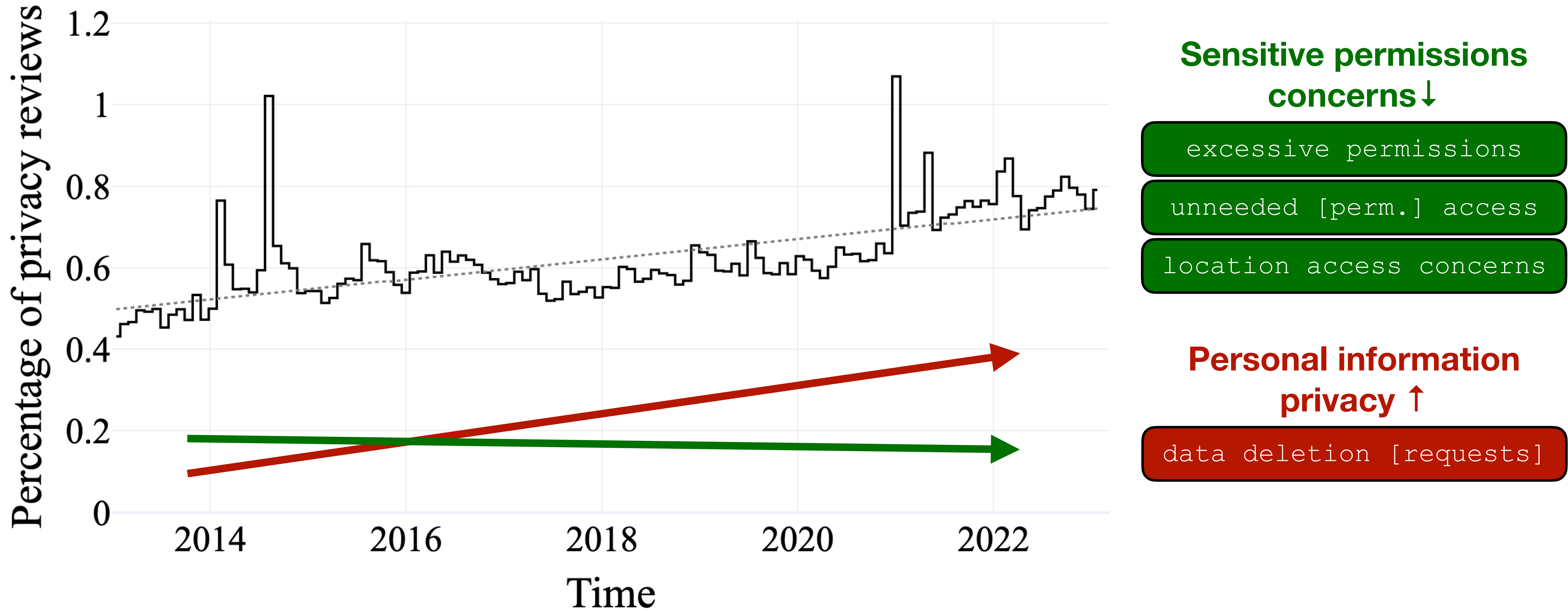
location access concerns

Personal information privacy ↑

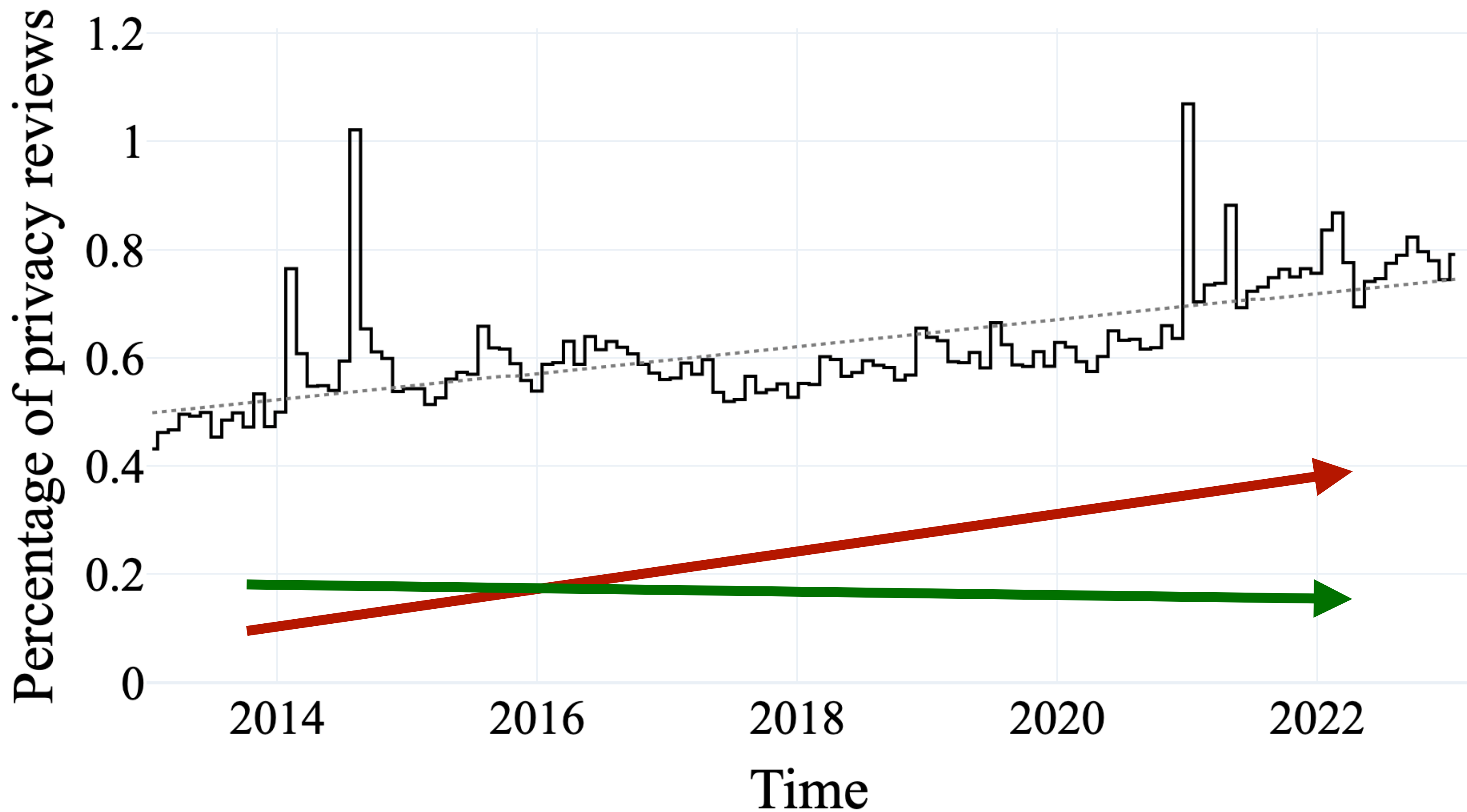
Themes change over time



Themes change over time



Themes change over time



Sensitive permissions concerns ↓

excessive permissions

unnneeded [perm.] access

location access concerns

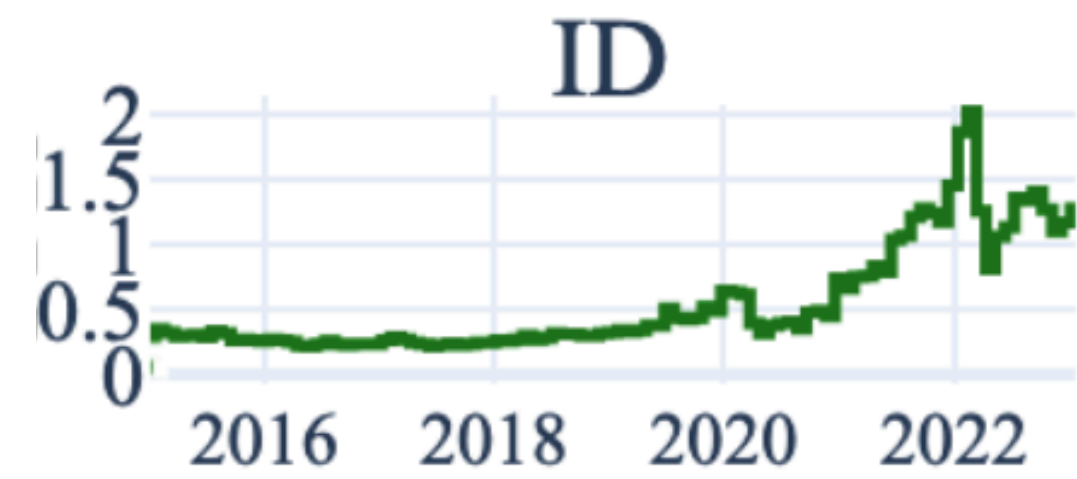
Personal information privacy ↑

data deletion [requests]

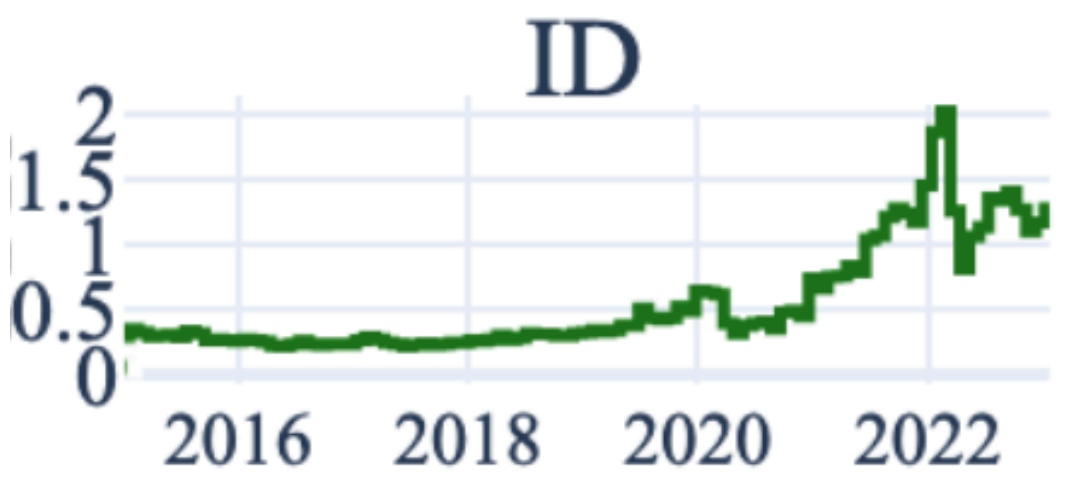
data theft

Ebbs and flows across countries

Ebbs and flows across countries



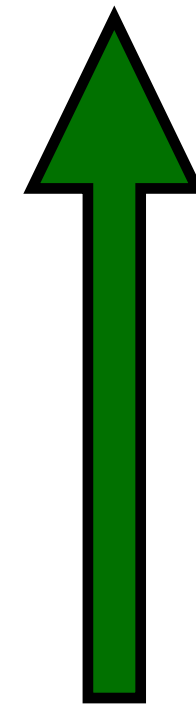
Ebbs and flows across countries



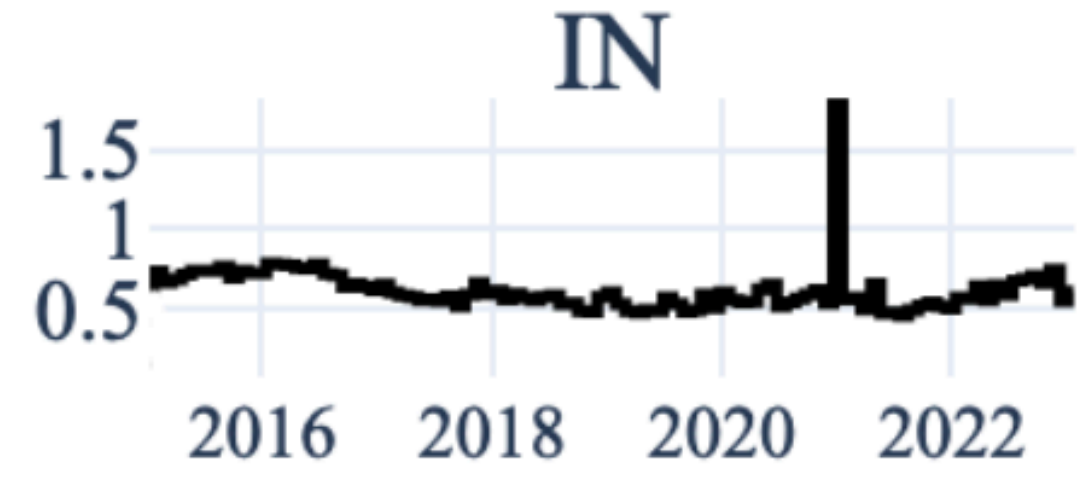
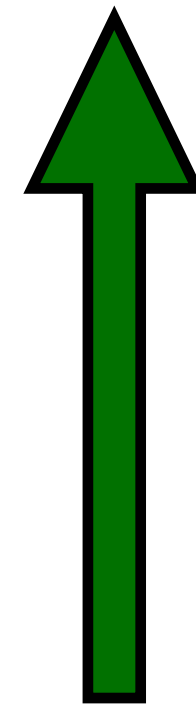
Ebbs and flows across countries



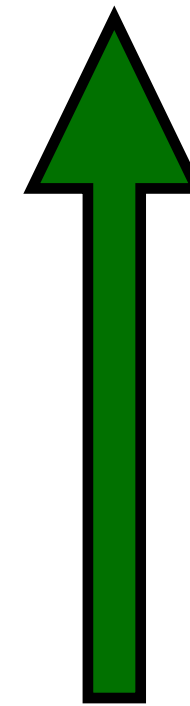
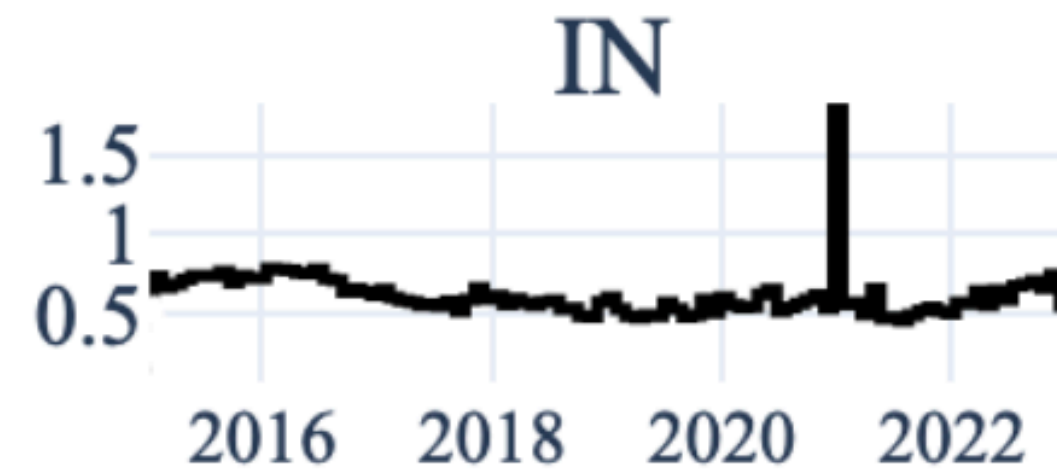
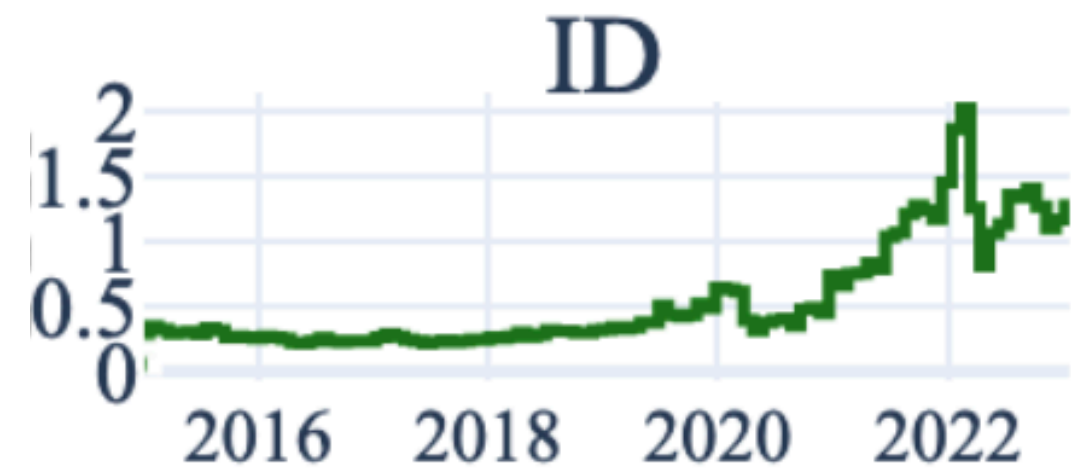
Ebbs and flows across countries



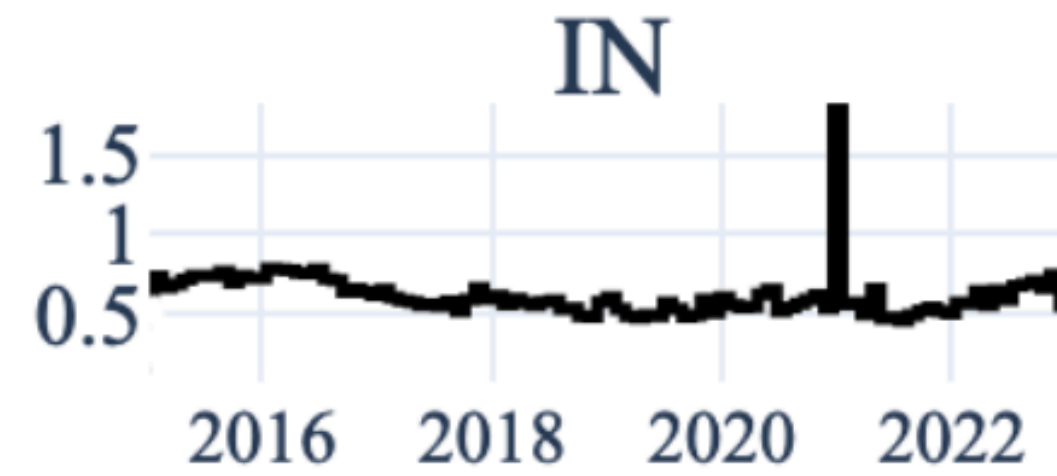
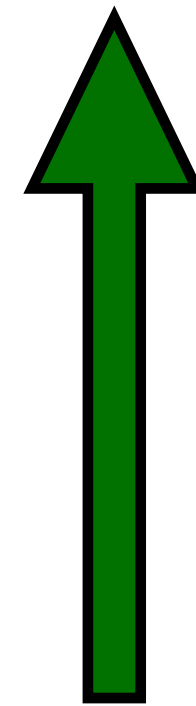
Ebbs and flows across countries



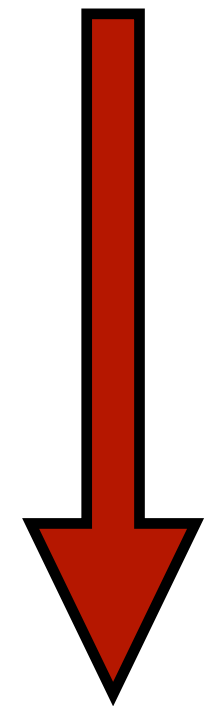
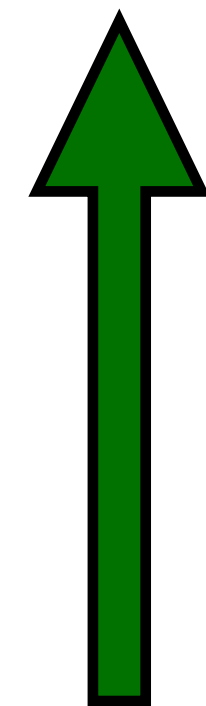
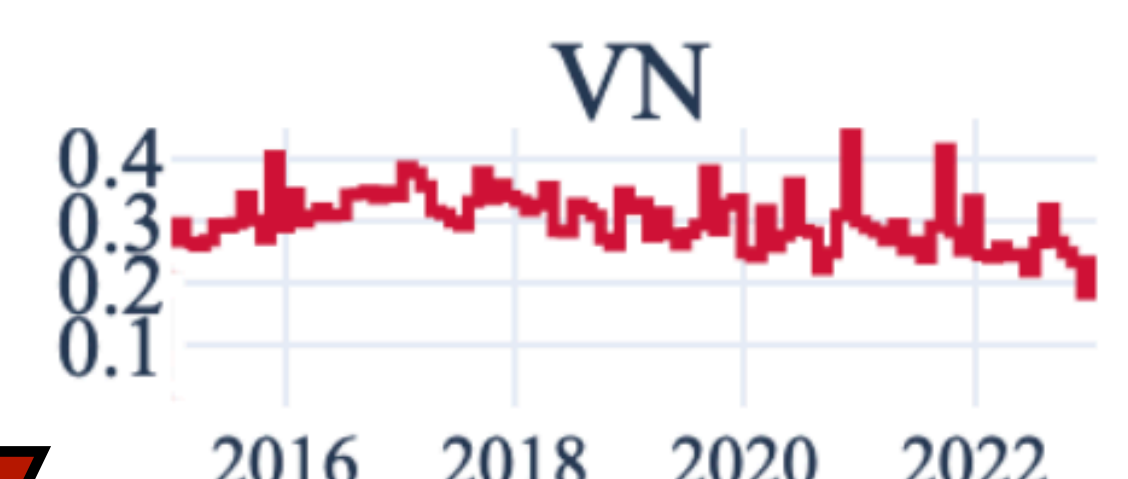
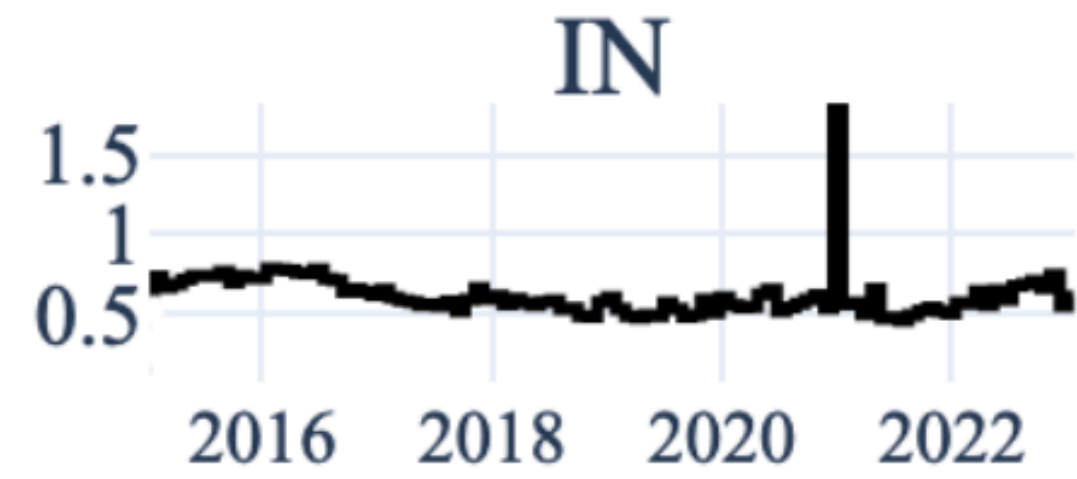
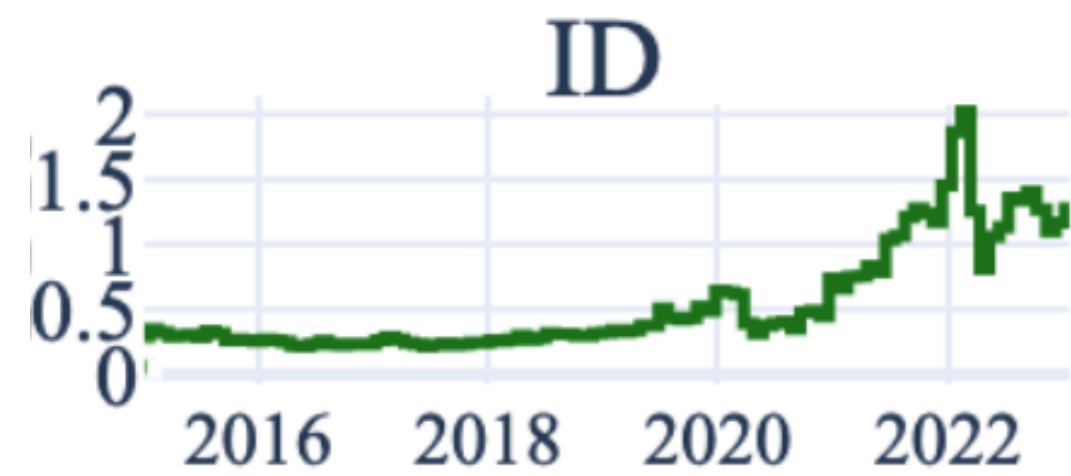
Ebbs and flows across countries



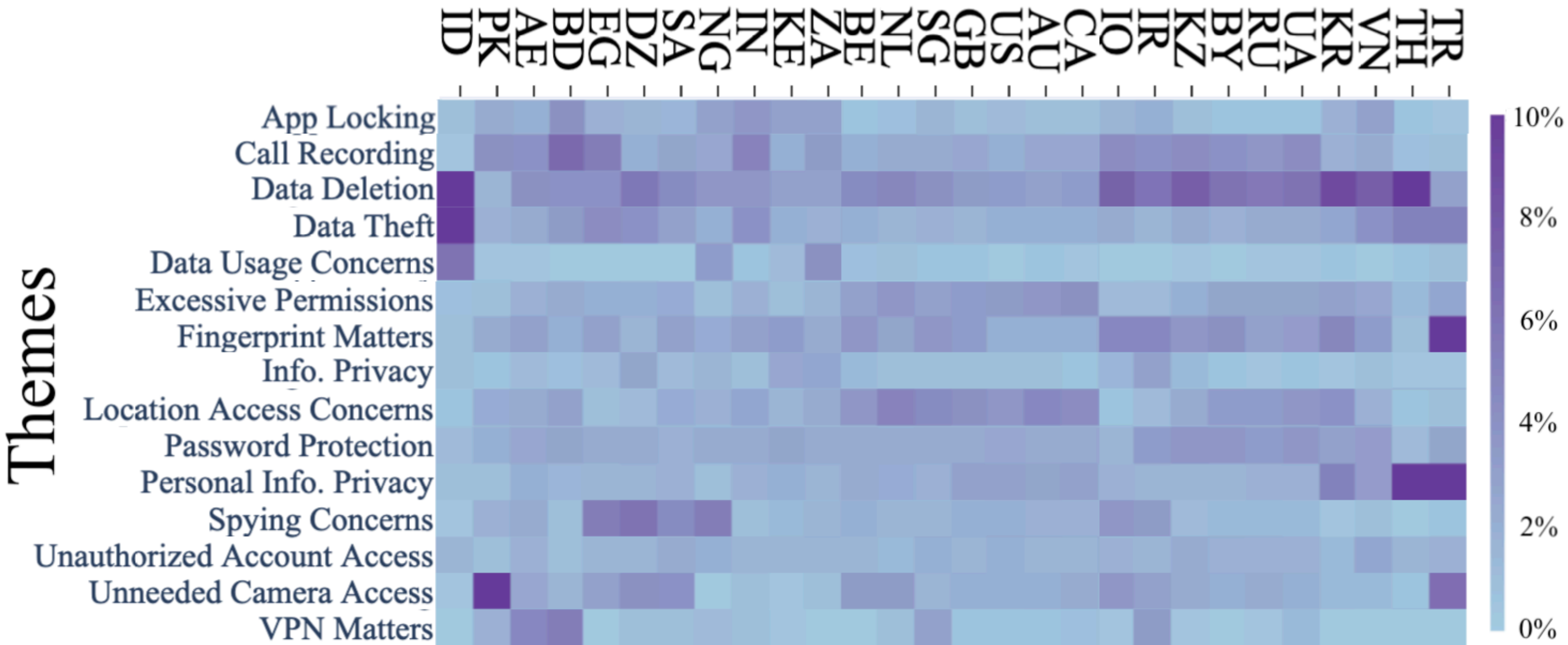
Ebbs and flows across countries



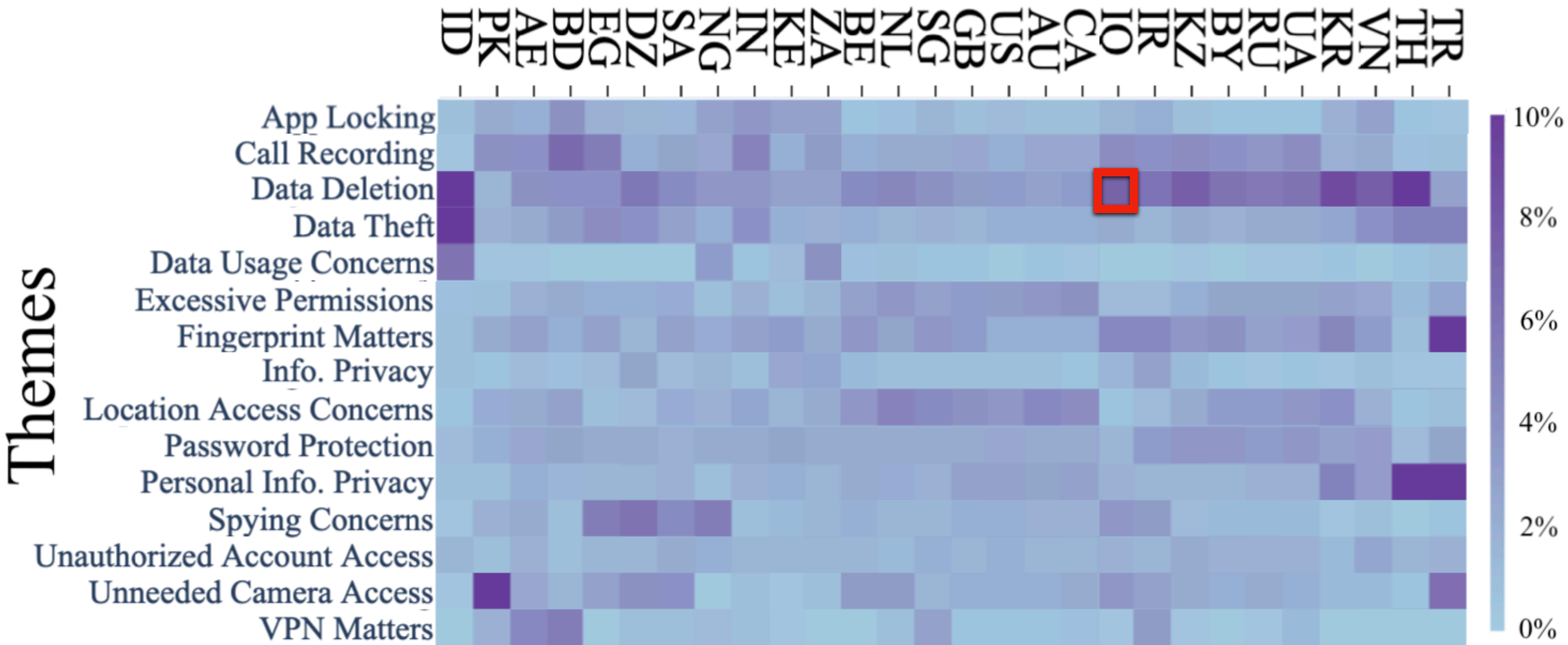
Ebbs and flows across countries



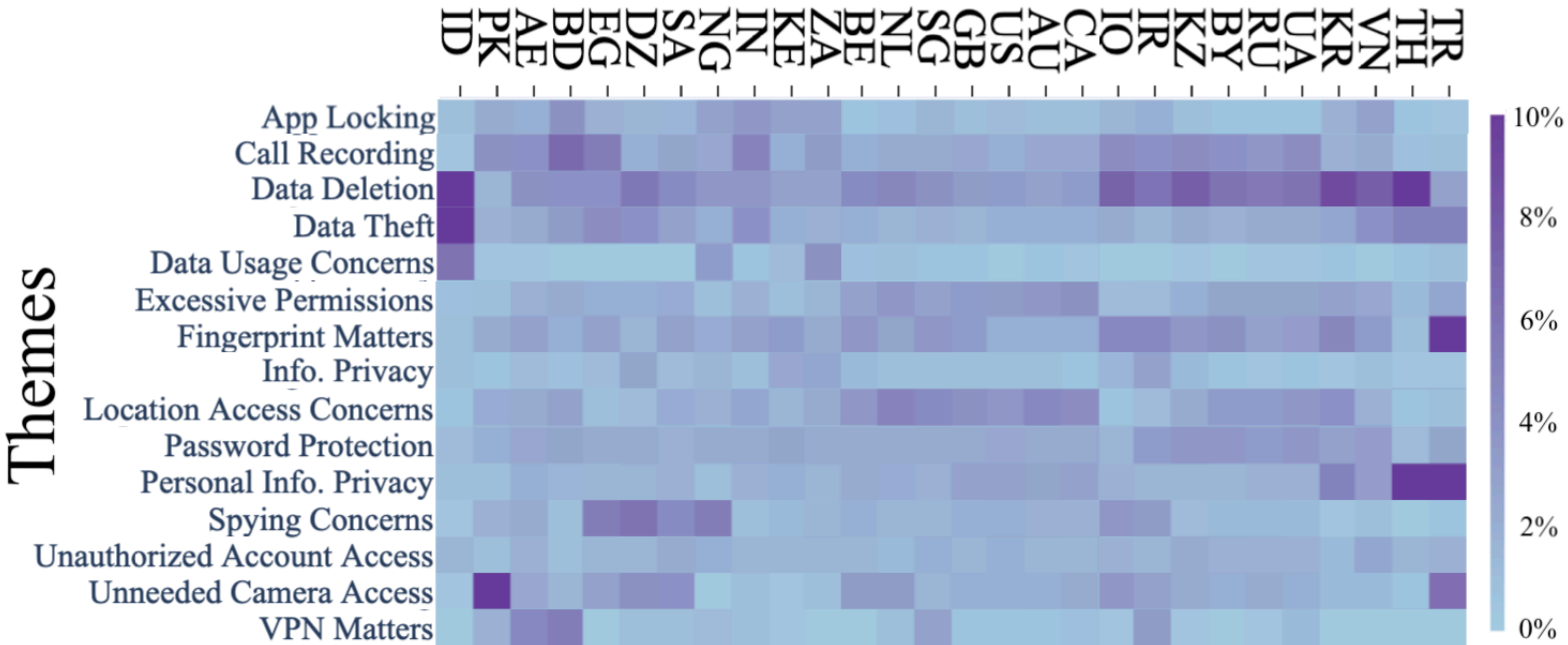
Countries



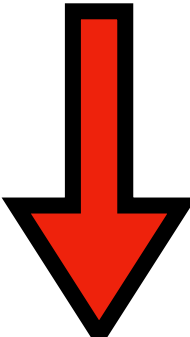
Countries



Countries

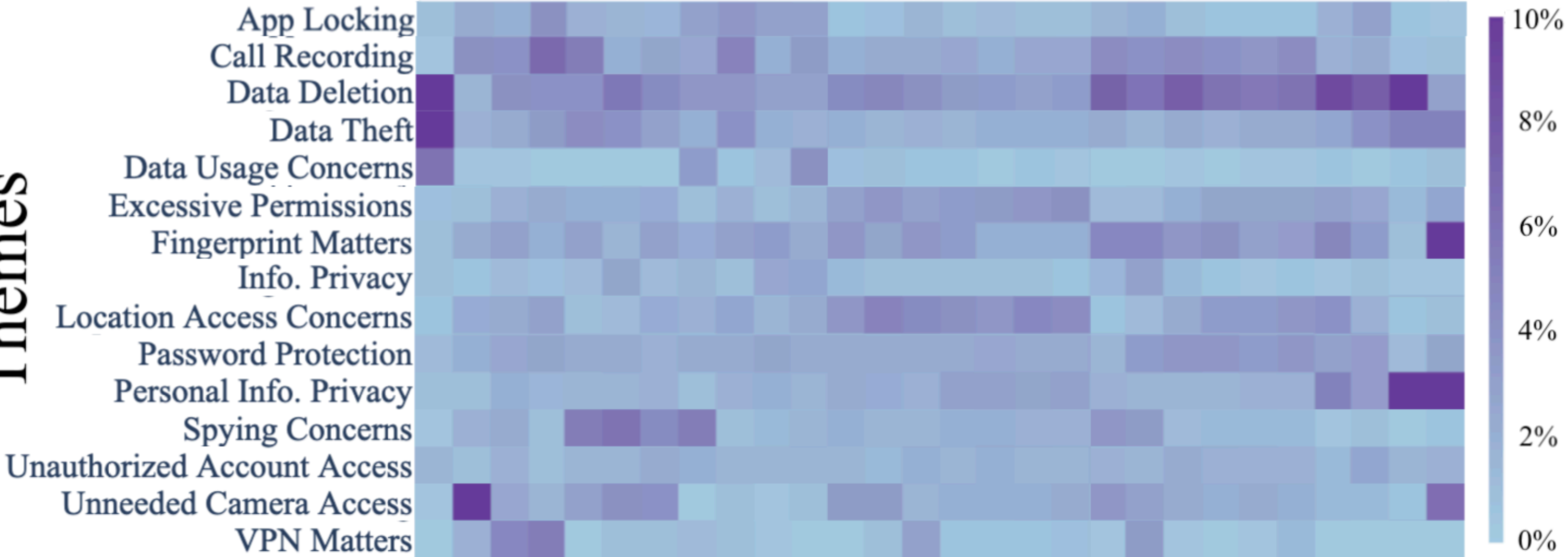


Countries

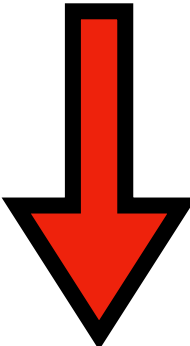


ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB US AD CA IO IR KZ BY RU UA KR VN TH TR

Themes

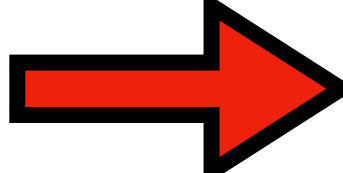


Countries

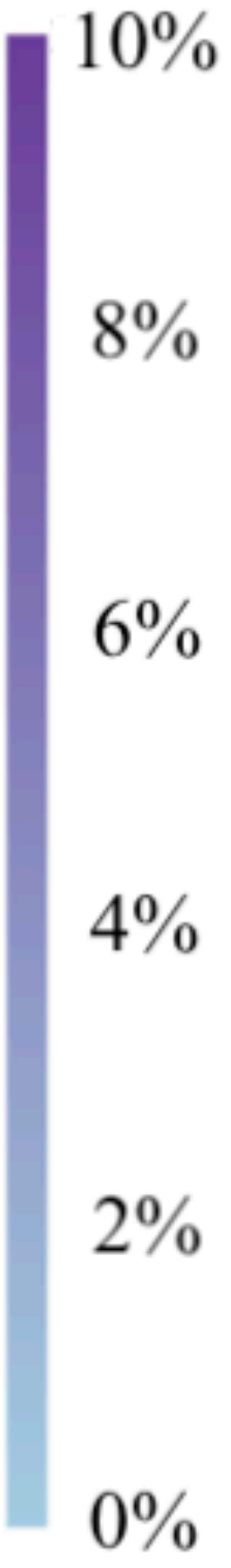


ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB US AD CA IO IR KZ BY RU UA KR VN TH TR

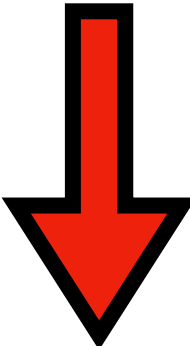
Themes



App Locking
Call Recording
Data Deletion
Data Theft
Data Usage Concerns
Excessive Permissions
Fingerprint Matters
Info. Privacy
Location Access Concerns
Password Protection
Personal Info. Privacy
Spying Concerns
Unauthorized Account Access
Unneeded Camera Access
VPN Matters

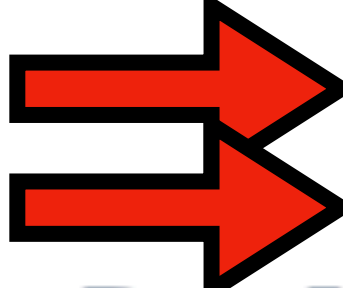


Countries

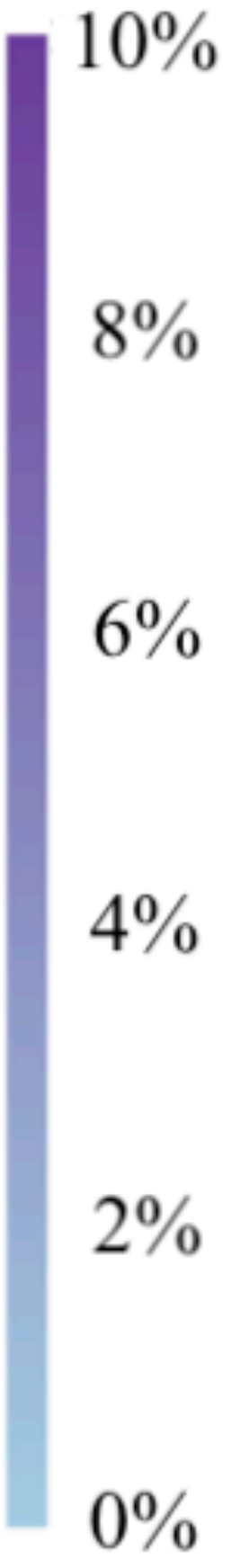


ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB US AD CA IO IR KZ BY RU UA KR VN TH TR

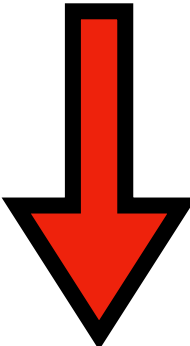
Themes



App Locking
Call Recording
Data Deletion
Data Theft
Data Usage Concerns
Excessive Permissions
Fingerprint Matters
Info. Privacy
Location Access Concerns
Password Protection
Personal Info. Privacy
Spying Concerns
Unauthorized Account Access
Unneeded Camera Access
VPN Matters

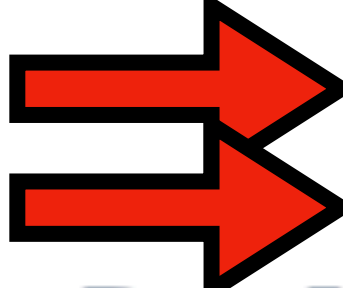


Countries

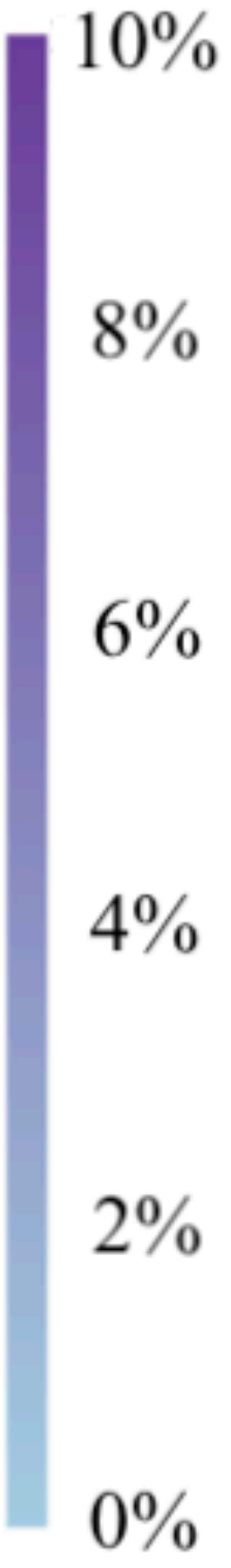


ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB US AD CA IO IR KZ BY RU UA KR VN TH TR

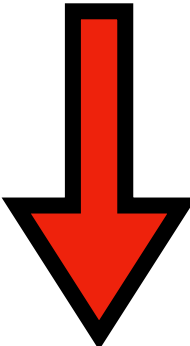
Themes



App Locking
Call Recording
Data Deletion
Data Theft
Data Usage Concerns
Excessive Permissions
Fingerprint Matters
Info. Privacy
Location Access Concerns
Password Protection
Personal Info. Privacy
Spying Concerns
Unauthorized Account Access
Unneeded Camera Access
VPN Matters

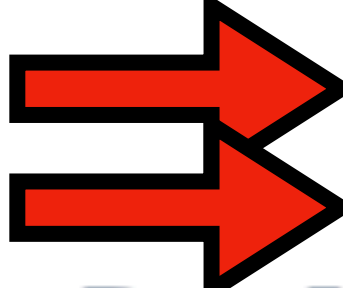


Countries

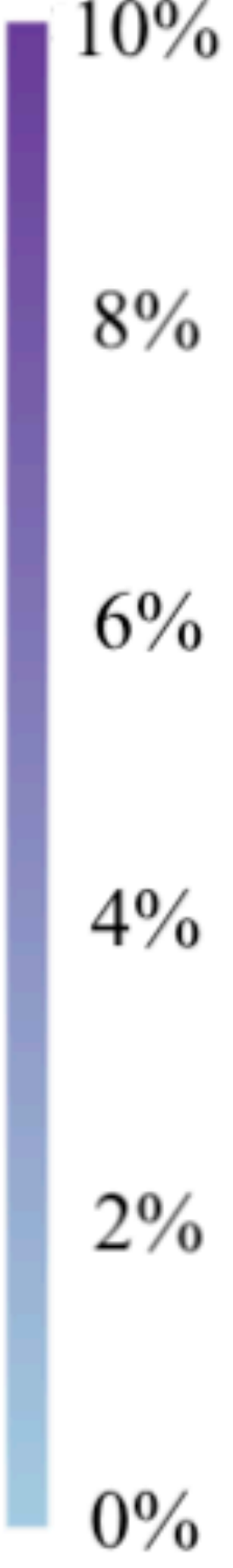
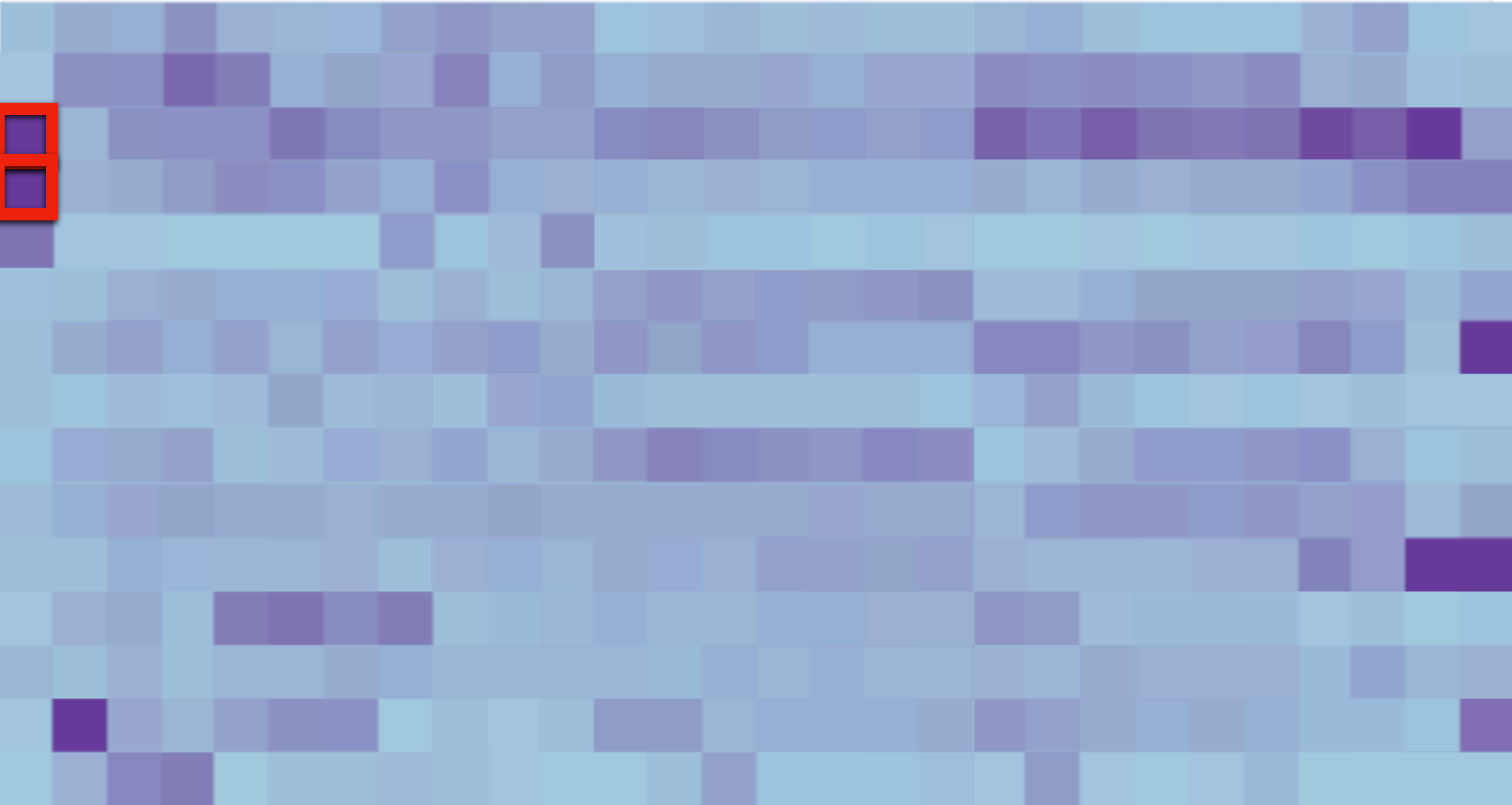


ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB US AD CA IO IR KZ BY RU UA KR VN TH TR

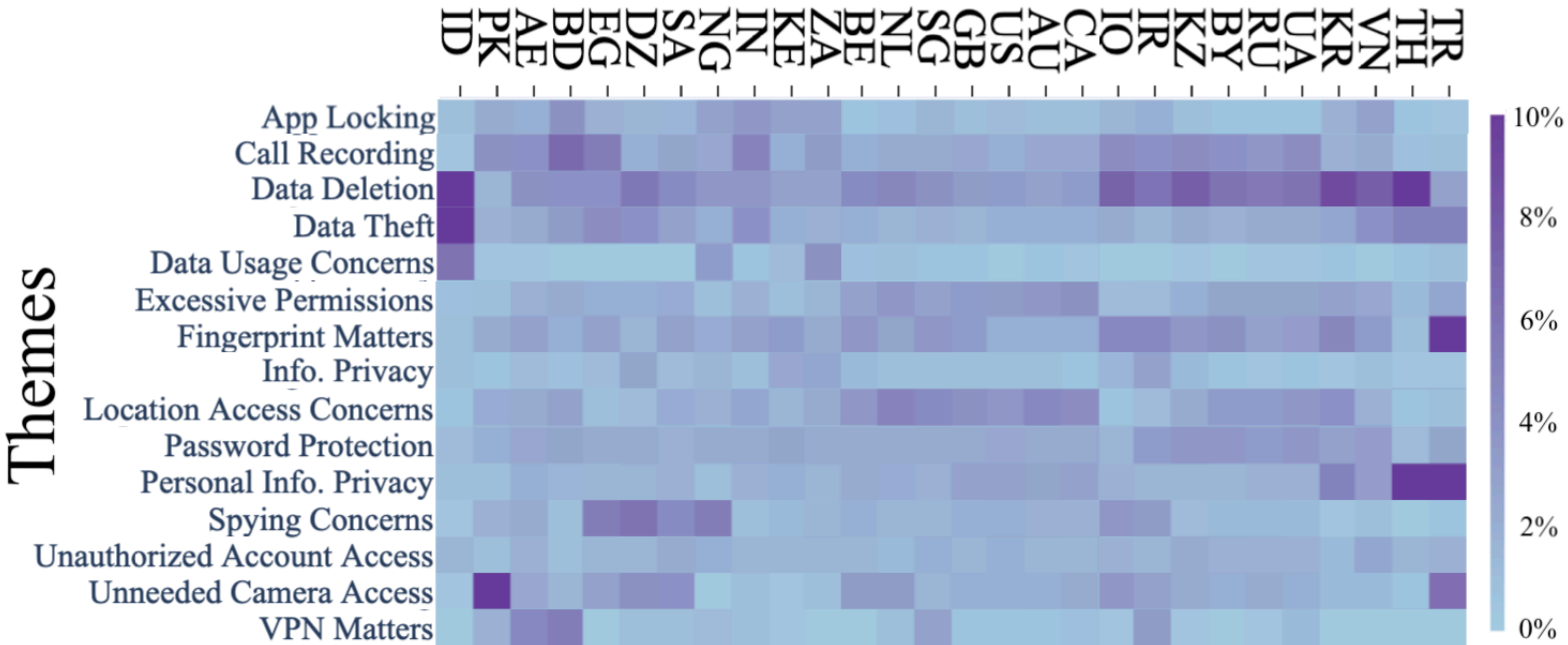
Themes



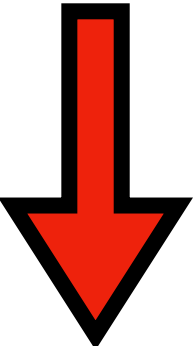
App Locking
Call Recording
Data Deletion
Data Theft
Data Usage Concerns
Excessive Permissions
Fingerprint Matters
Info. Privacy
Location Access Concerns
Password Protection
Personal Info. Privacy
Spying Concerns
Unauthorized Account Access
Unneeded Camera Access
VPN Matters



Countries

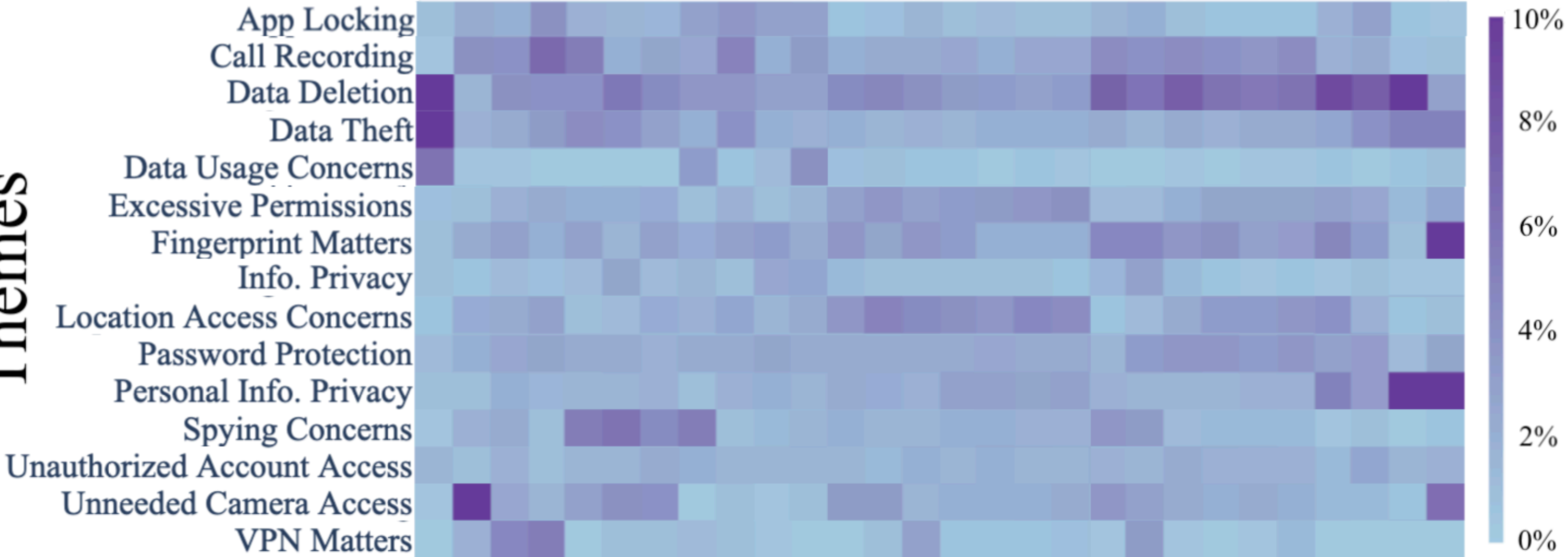


Countries

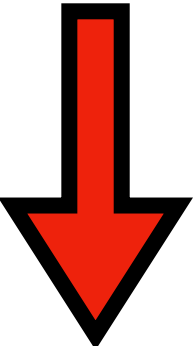


ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB US AD CA IO IR KZ BY RU UA KR VN TH TR

Themes

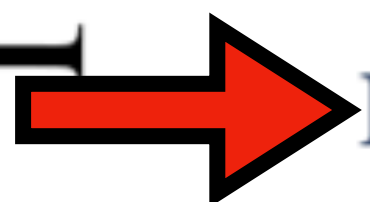
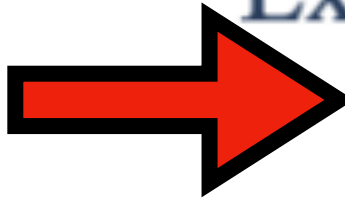


Countries

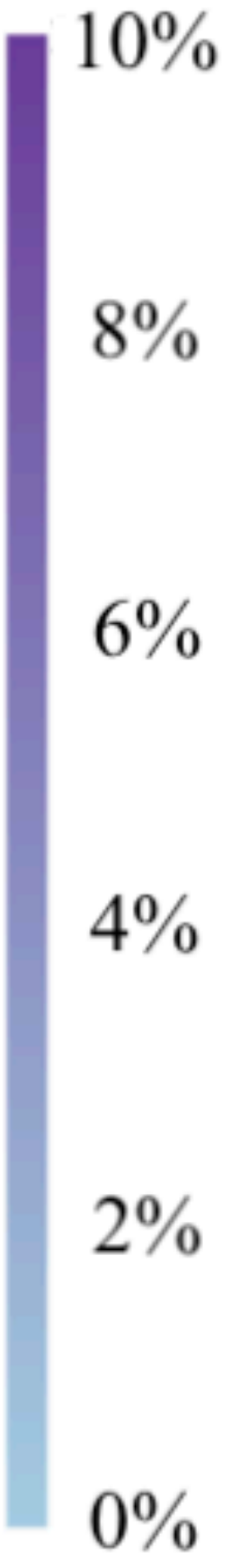


ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB AD CA IO IR KZ BY RU UA KR VN TH TR

Themes



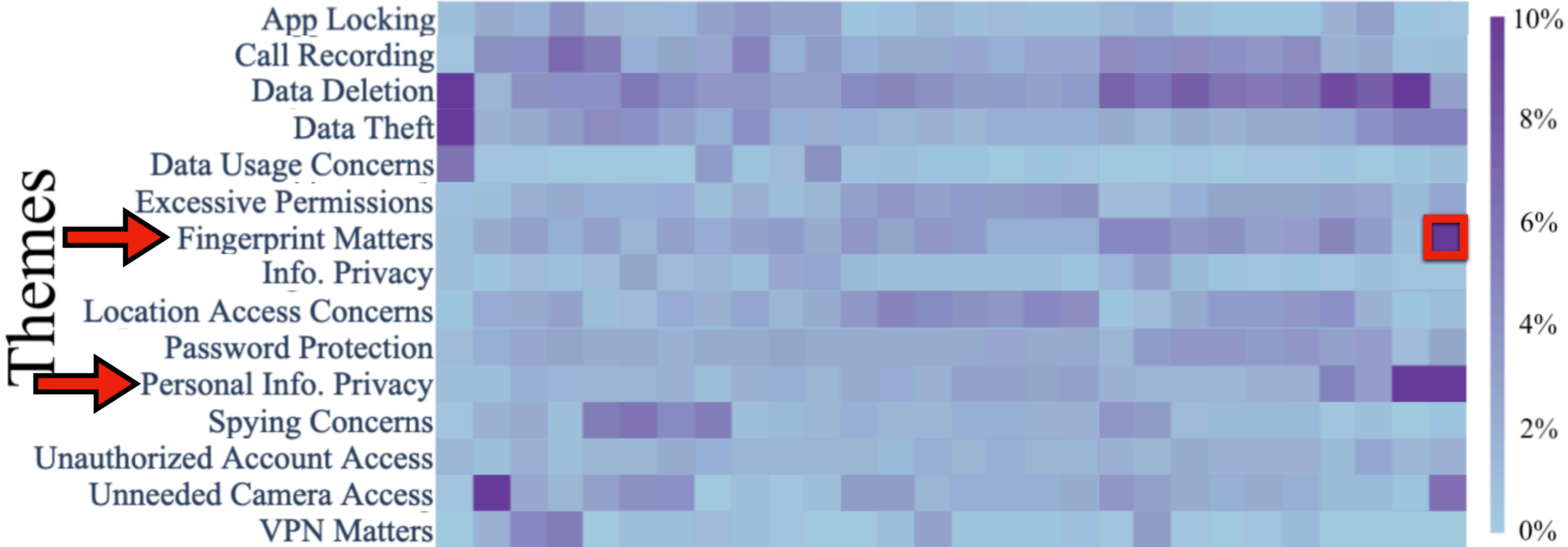
App Locking
Call Recording
Data Deletion
Data Theft
Data Usage Concerns
Excessive Permissions
Fingerprint Matters
Info. Privacy
Location Access Concerns
Password Protection
Personal Info. Privacy
Spying Concerns
Unauthorized Account Access
Unneeded Camera Access
VPN Matters



Countries

ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB US AD CA IO IR KZ BY RU UA KR VN TH TR

Themes



Countries


ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB US AD CA IO IR KZ BY RU UA KR VN TH TR

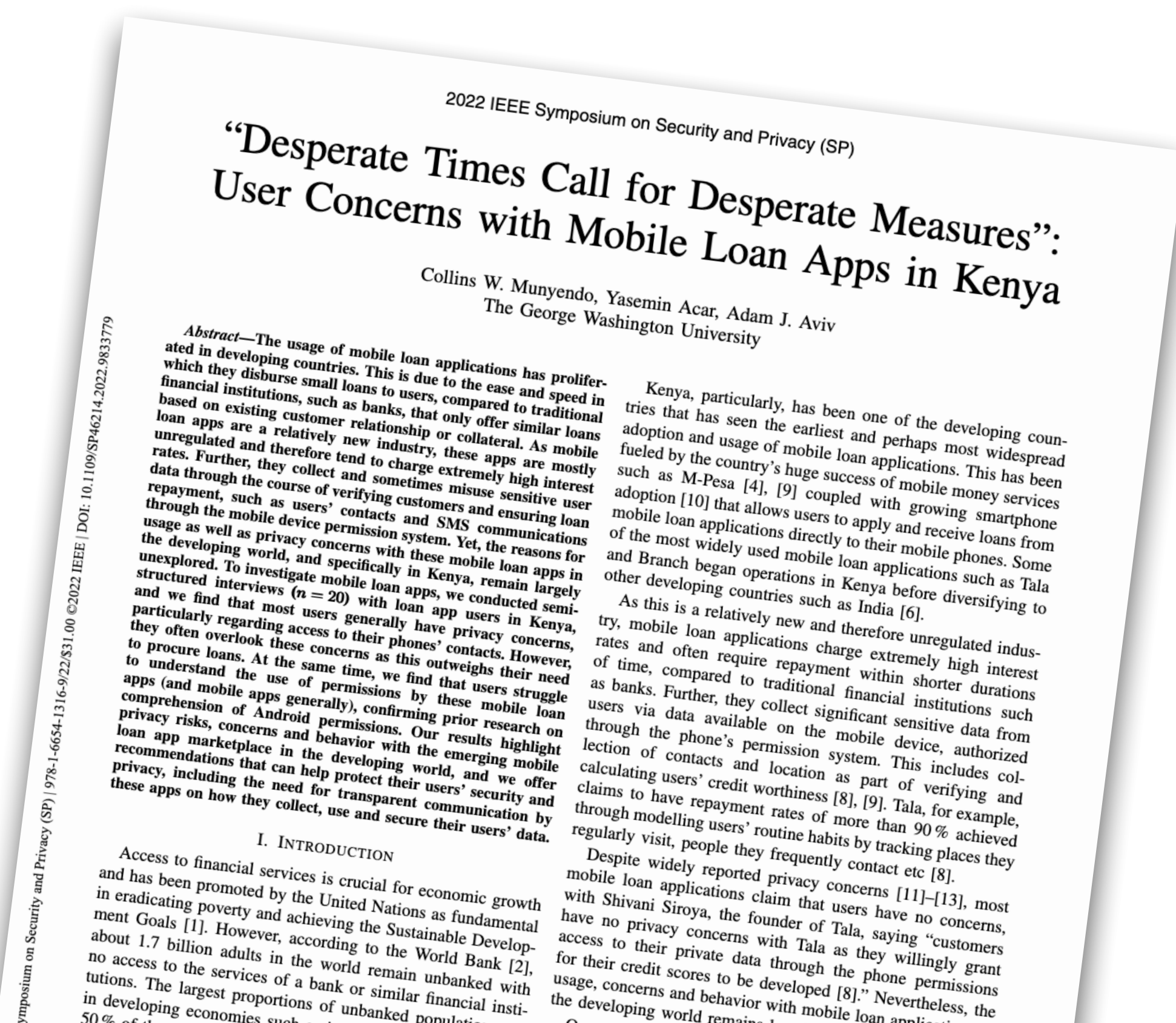
Themes



Predatory loan apps: they're global :(

Predatory loan apps: they're global :(

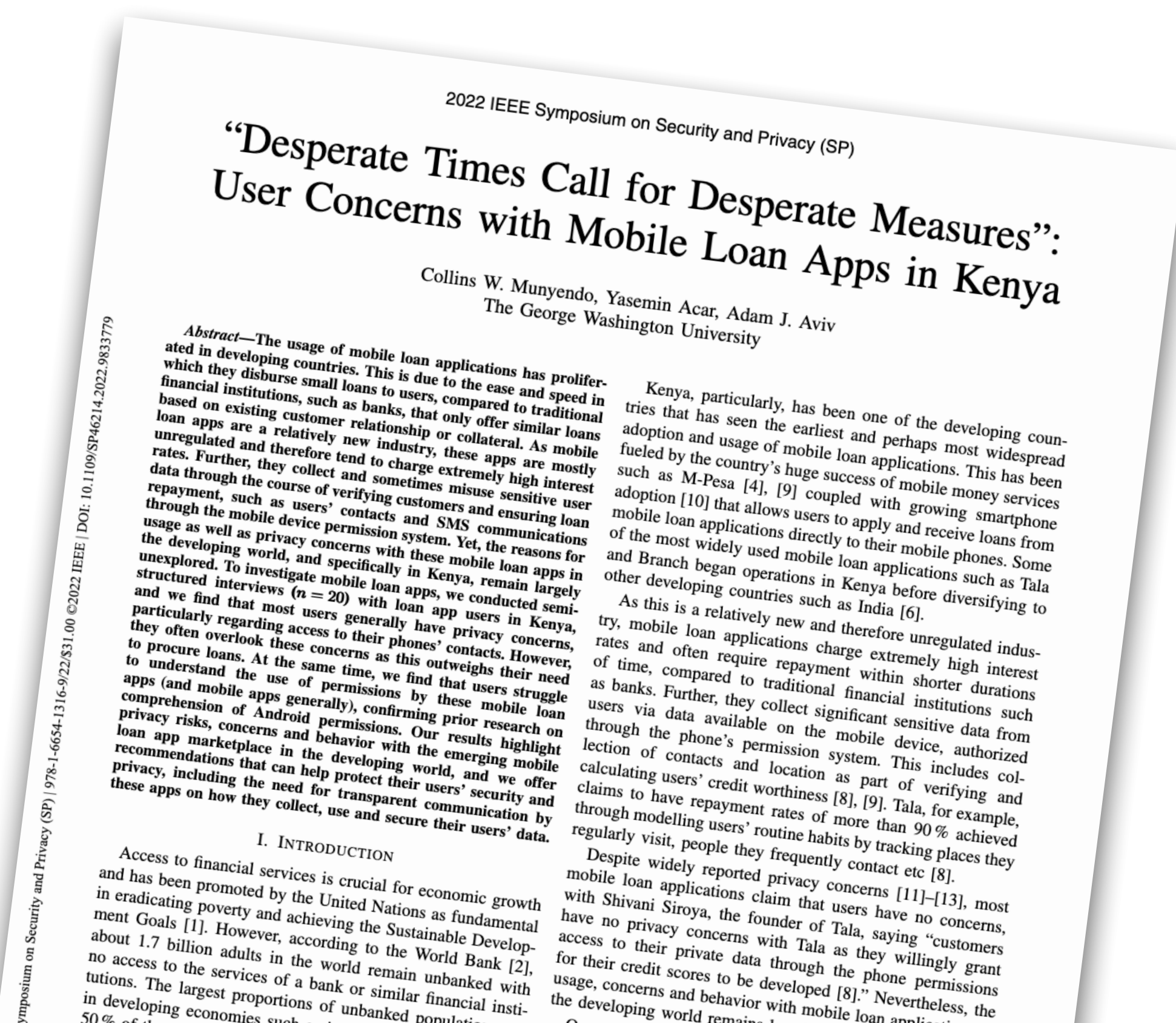
- Prior work: loan apps highly privacy invasive. 




Predatory loan apps: they're global :(

data deletion

- Prior work: loan apps highly privacy invasive. 🇰🇪



Predatory loan apps: they're global :(

- Prior work: loan apps highly privacy invasive. 

data deletion

data theft

“Desperate Times Call for Desperate Measures”: User Concerns with Mobile Loan Apps in Kenya

Collins W. Munyendo, Yasemin Acar, Adam J. Aviv
The George Washington University

Abstract—The usage of mobile loan applications has proliferated in developing countries. This is due to the ease and speed in which they disburse small loans to users, compared to traditional financial institutions, such as banks, that only offer similar loans based on existing customer relationship or collateral. As mobile loan apps are a relatively new industry, these apps are mostly unregulated and therefore tend to charge extremely high interest rates. Further, they collect and sometimes misuse sensitive user data through the course of verifying customers and ensuring loan repayment, such as users’ contacts and SMS communications through the mobile device permission system. Yet, the reasons for the developing world, and specifically in Kenya, remain largely unexplored. To investigate mobile loan apps, we conducted structured interviews ($n = 20$) with loan app users in Kenya, and we find that most users generally have privacy concerns, particularly regarding access to their phones’ contacts. However, they often overlook these concerns as this outweighs their need to procure loans. At the same time, we find that users struggle to understand the use of permissions by these mobile loan apps (and mobile apps generally), confirming prior research on comprehension of Android permissions. Our results highlight privacy risks, concerns and behavior with the emerging mobile loan app marketplace in the developing world, and we offer recommendations that can help protect their users’ security and privacy, including the need for transparent communication by these apps on how they collect, use and secure their users’ data.

I. INTRODUCTION


Access to financial services is crucial for economic growth and has been promoted by the United Nations as fundamental in eradicating poverty and achieving the Sustainable Development Goals [1]. However, according to the World Bank [2], about 1.7 billion adults in the world remain unbanked with no access to the services of a bank or similar financial institutions. The largest proportions of unbanked population in developing economies such as Kenya are women, with 50% of the population being unbanked.

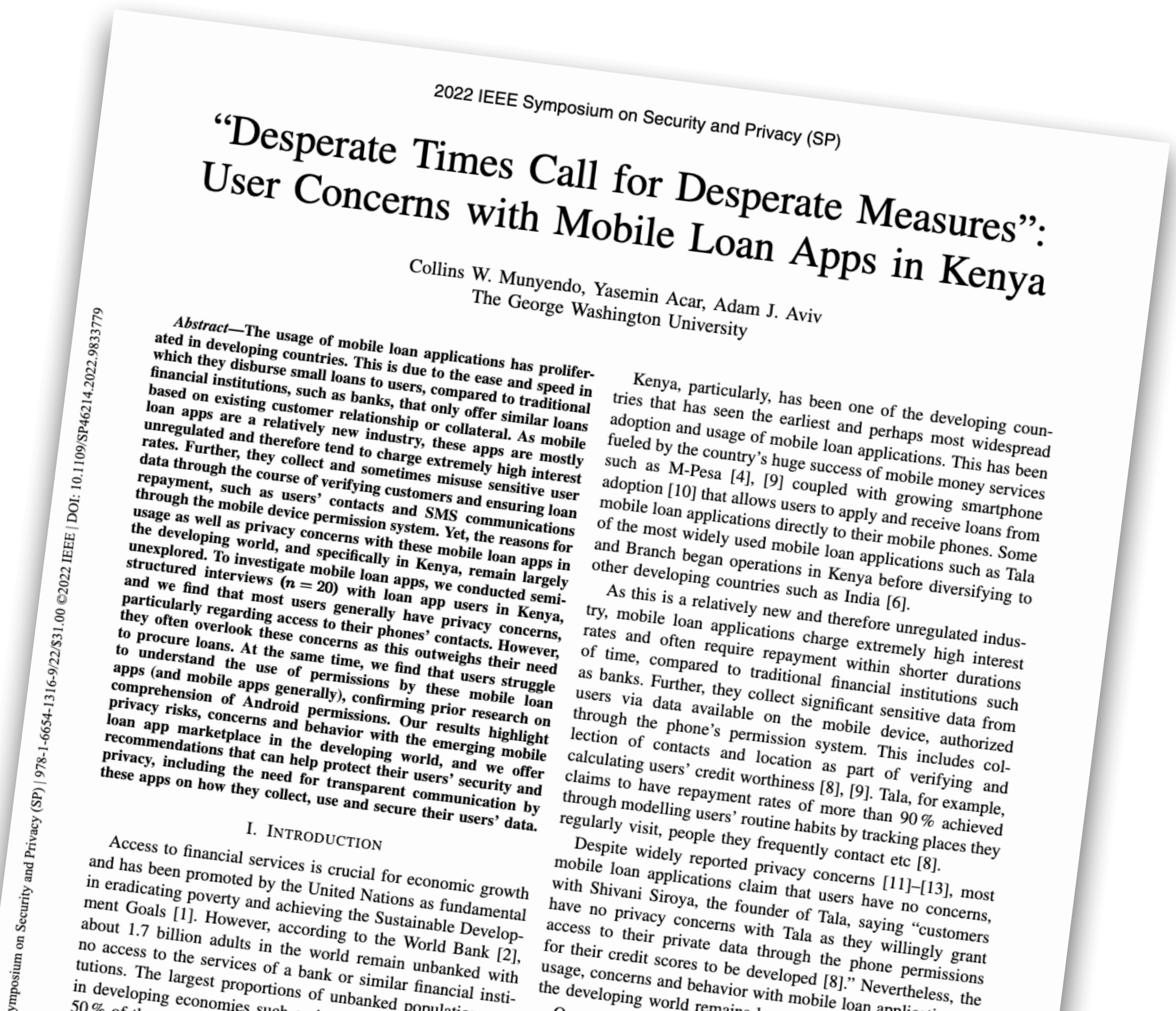
Kenya, particularly, has been one of the developing countries that has seen the earliest and perhaps most widespread adoption and usage of mobile loan applications. This has been fueled by the country’s huge success of mobile money services such as M-Pesa [4], [9] coupled with growing smartphone adoption [10] that allows users to apply and receive loans from mobile loan applications directly to their mobile phones. Some of the most widely used mobile loan applications such as Tala and Branch began operations in Kenya before diversifying to other developing countries such as India [6].

As this is a relatively new and therefore unregulated industry, mobile loan applications charge extremely high interest rates and often require repayment within shorter durations of time, compared to traditional financial institutions such as banks. Further, they collect significant sensitive data from users via data available on the mobile device, authorized through the phone’s permission system. This includes collection of contacts and location as part of verifying and calculating users’ credit worthiness [8], [9]. Tala, for example, claims to have repayment rates of more than 90% achieved through modelling users’ routine habits by tracking places they regularly visit, people they frequently contact etc [8].

Despite widely reported privacy concerns [11]–[13], most mobile loan applications claim that users have no concerns, with Shivani Siroya, the founder of Tala, saying “customers have no privacy concerns with Tala as they willingly grant access to their private data through the phone permissions for their credit scores to be developed [8].” Nevertheless, the usage, concerns and behavior with mobile loan applications in the developing world remain largely unexplored.

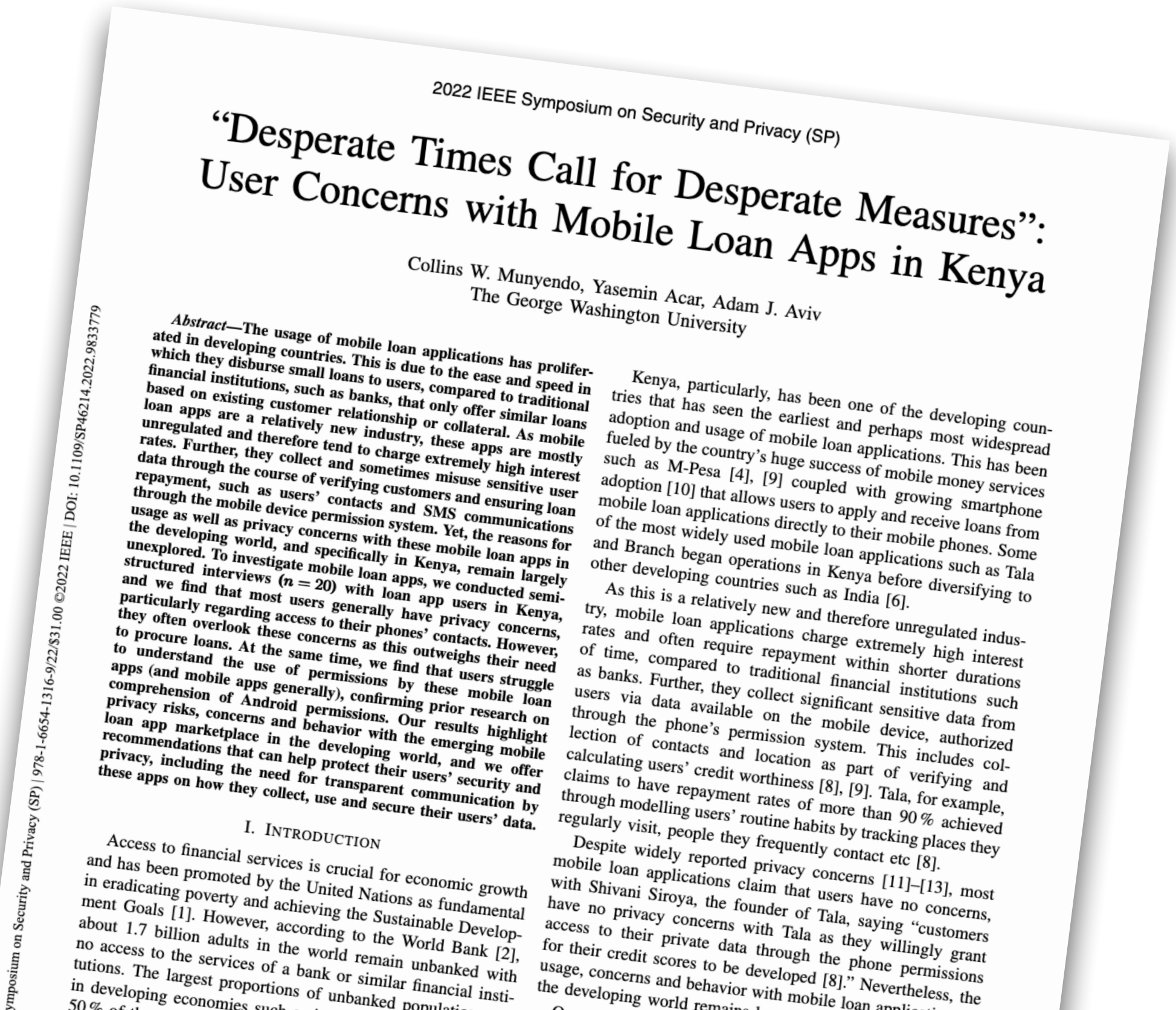
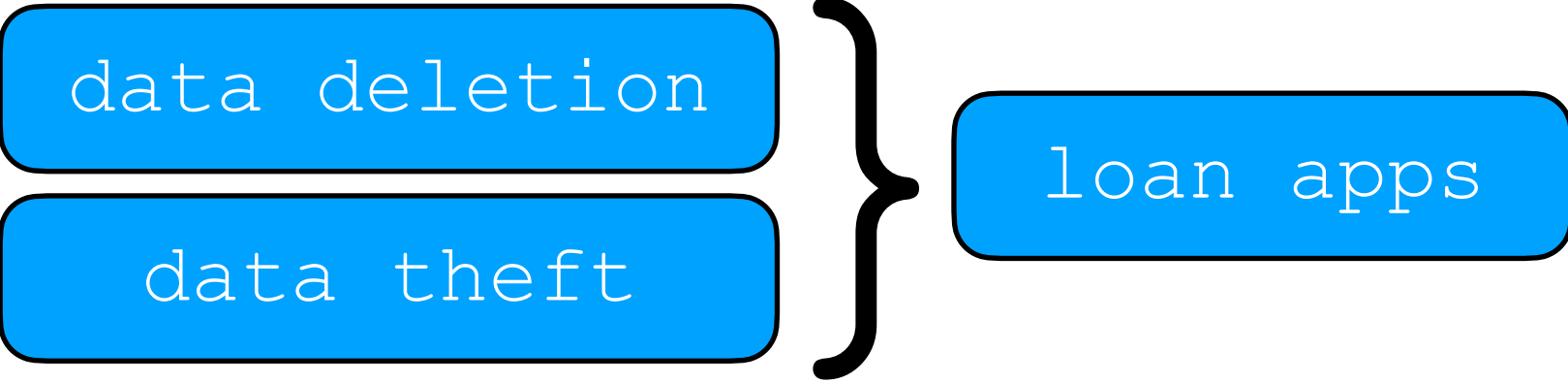
Predatory loan apps: they're global :(

- Prior work: loan apps highly privacy invasive. 




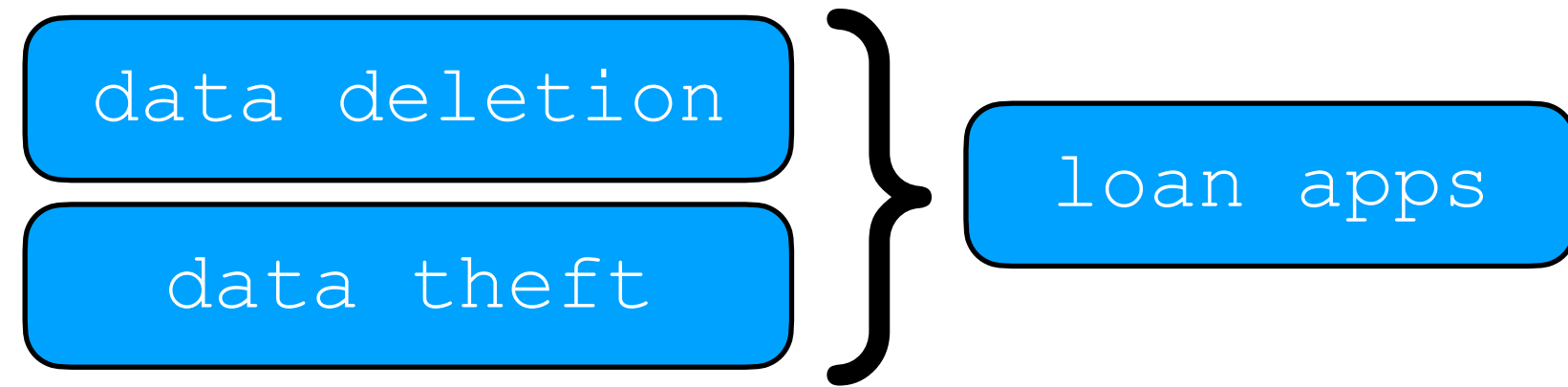
Predatory loan apps: they're global :(

- Prior work: loan apps highly privacy invasive. 

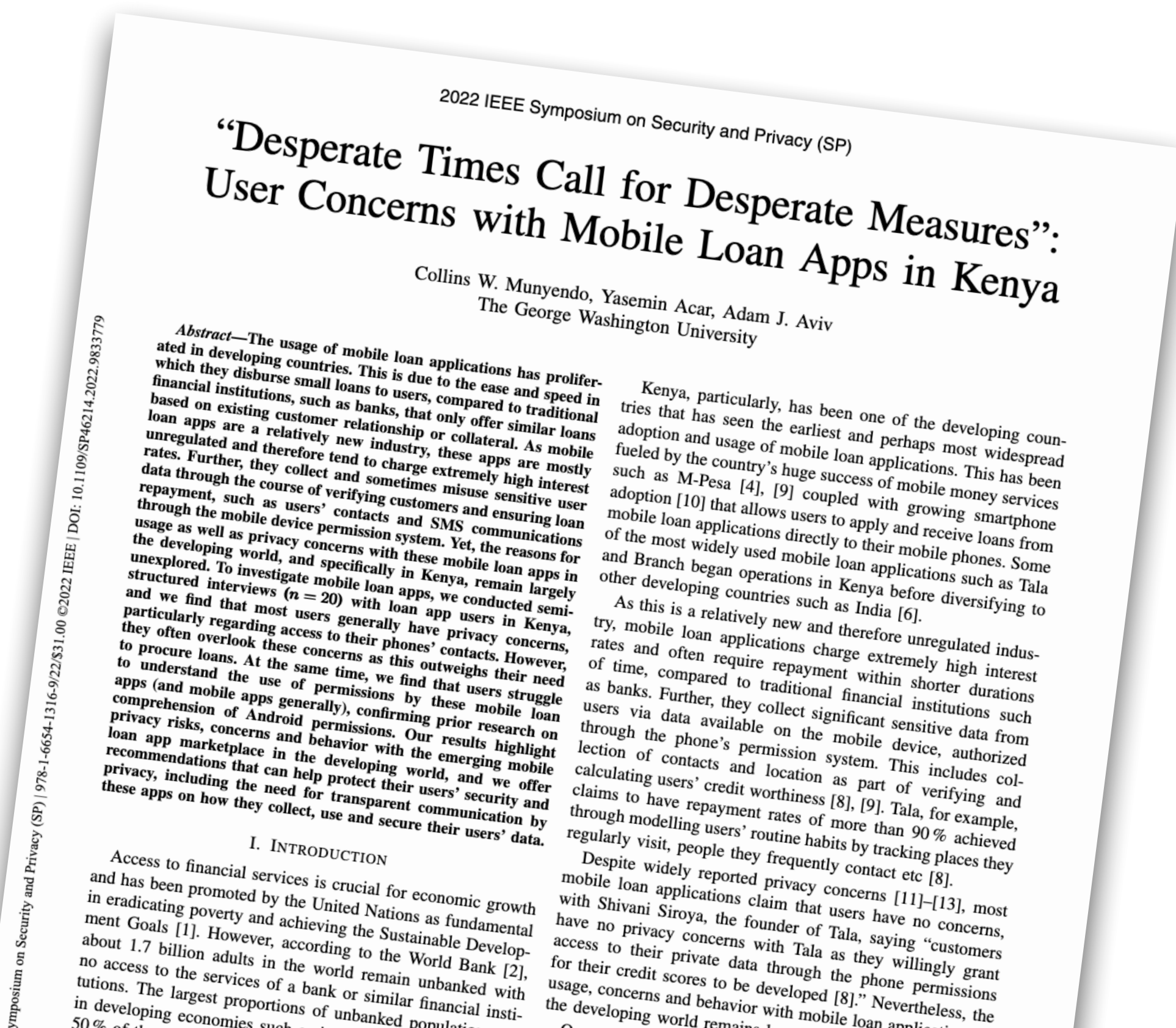


Predatory loan apps: they're global :(

- Prior work: loan apps highly privacy invasive. 

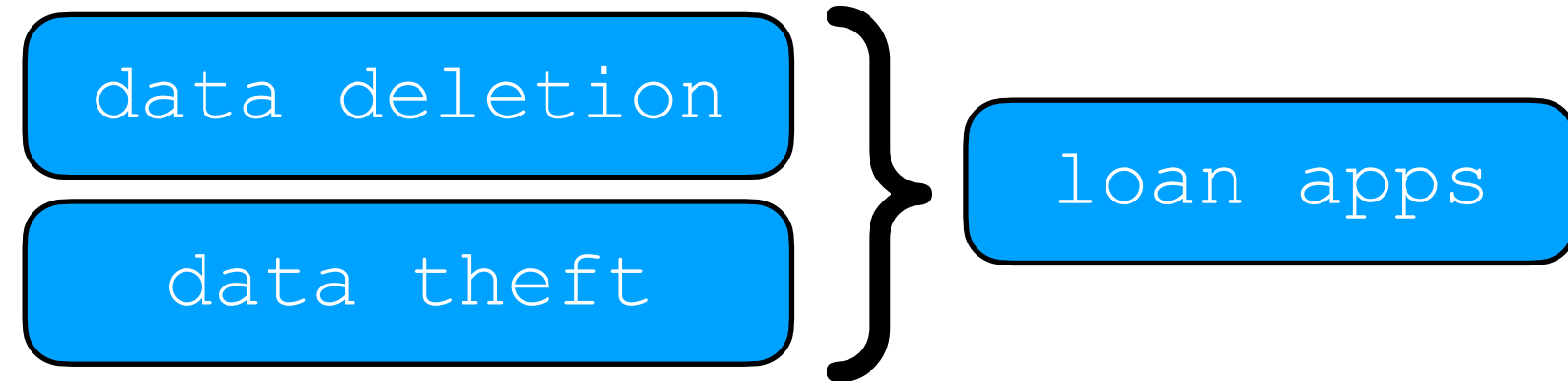


- Loan complaints in: Indonesia , India , Mexico , and more

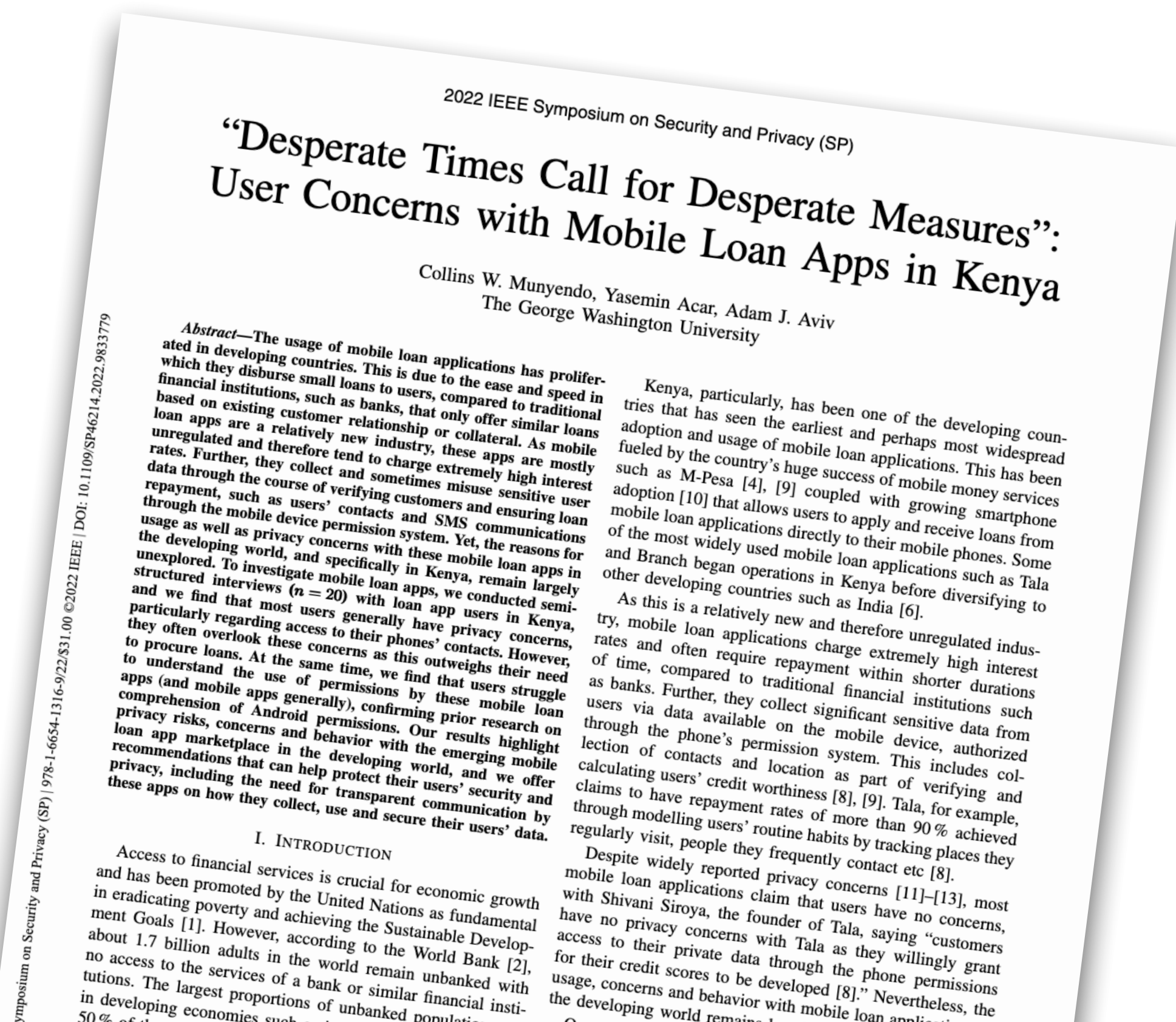


Predatory loan apps: they're global :(

- Prior work: loan apps highly privacy invasive. 🇰🇪

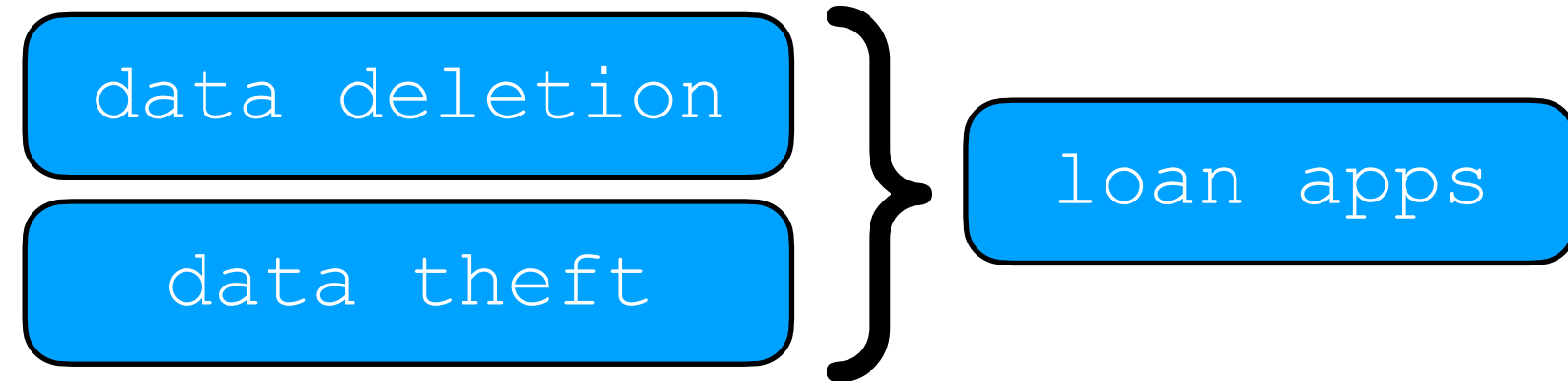


- Loan complaints in: Indonesia 🇮🇩, India 🇮🇳, Mexico 🇲🇽, and more



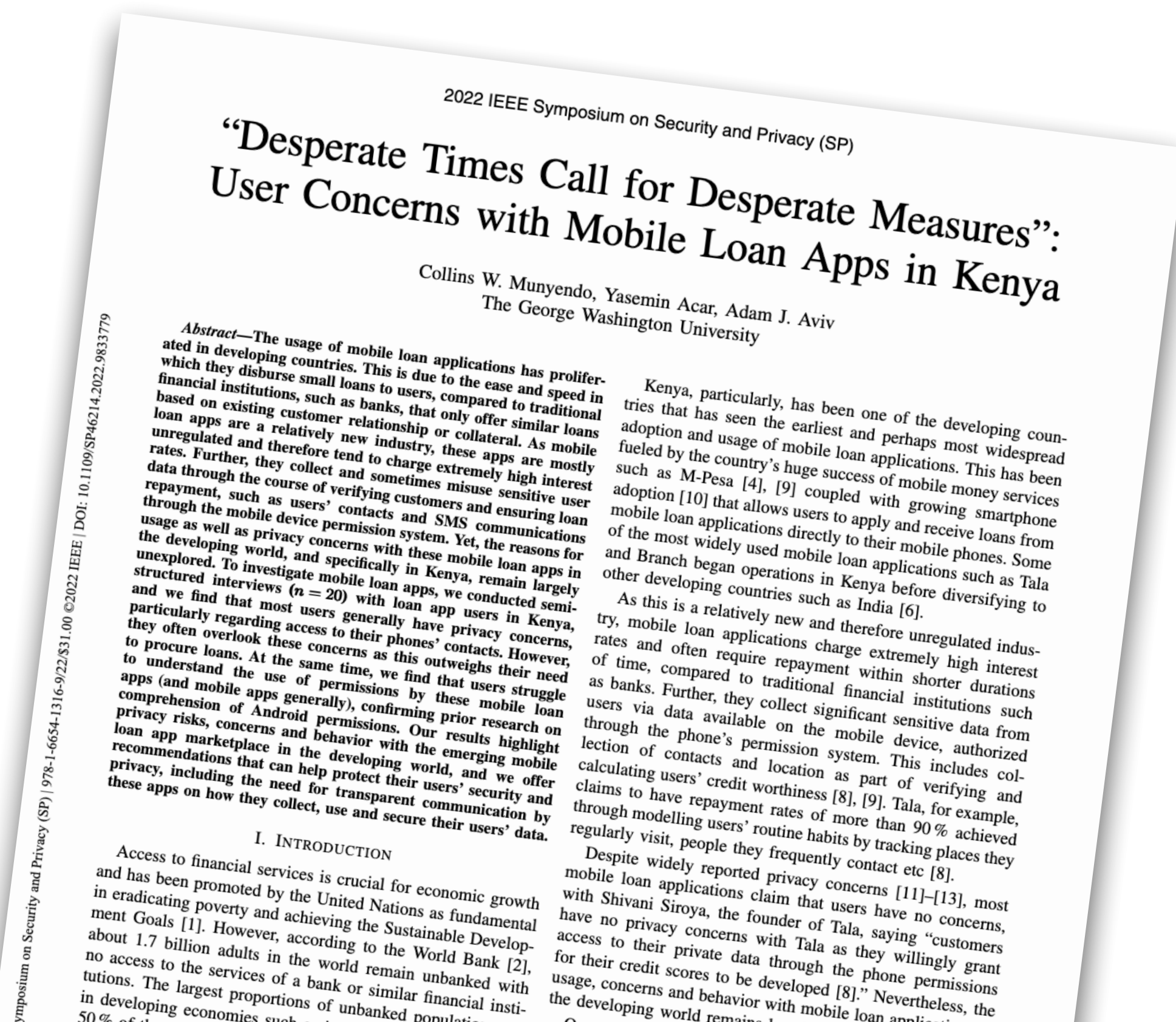
Predatory loan apps: they're global :(

- Prior work: loan apps highly privacy invasive. 🇰🇪




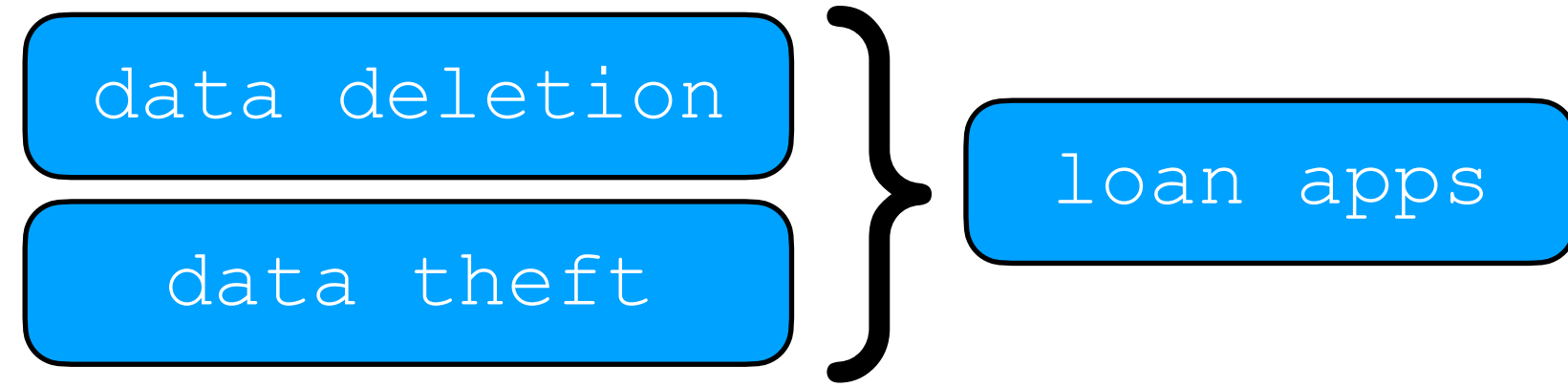
- Loan complaints in:
Indonesia 🇮🇩,
India 🇮🇳,
Mexico 🇲🇽,
and more

The app stole my data, including my facebook account. It told me that the loan process would be easier if I input all of my data.



Predatory loan apps: they're global :(

- Prior work: loan apps highly privacy invasive. 



- Loan complaints in: Indonesia , India , Mexico , and more

The app stole my data, including my facebook account. It told me that the loan process would be easier if I input all of my data.



2022 IEEE Symposium on Security and Privacy (SP)
 “Desperate Times Call for Desperate Measures”:
 User Concerns with Mobile Loan Apps in Kenya
 Collins W. Munyendo, Yasemin Acar, Adam J. Aviv
 The George Washington University

Abstract—The usage of mobile loan applications has proliferated in developing countries. This is due to the ease and speed in which they disburse small loans to users, compared to traditional financial institutions, such as banks, that only offer similar loans based on existing customer relationship or collateral. As mobile loan apps are a relatively new industry, these apps are mostly unregulated and therefore tend to charge extremely high interest rates. Further, they collect and sometimes misuse sensitive user data through the course of verifying customers and ensuring loan repayment, such as users’ contacts and SMS communications through the mobile device permission system. Yet, the reasons for the developing world, and specifically in Kenya, remain largely unexplored. To investigate mobile loan apps, we conducted structured interviews (n = 20) with loan app users in Kenya, and we find that most users generally have privacy concerns, particularly regarding access to their phones’ contacts. However, they often overlook these concerns as this outweighs their need to procure loans. At the same time, we find that users struggle to understand the use of permissions by these mobile loan apps (and mobile apps generally), confirming prior research on comprehension of Android permissions. Our results highlight privacy risks, concerns and behavior with the emerging mobile loan app marketplace in the developing world, and we offer recommendations that can help protect their users’ security and privacy, including the need for transparent communication by these apps on how they collect, use and secure their users’ data.

I. INTRODUCTION

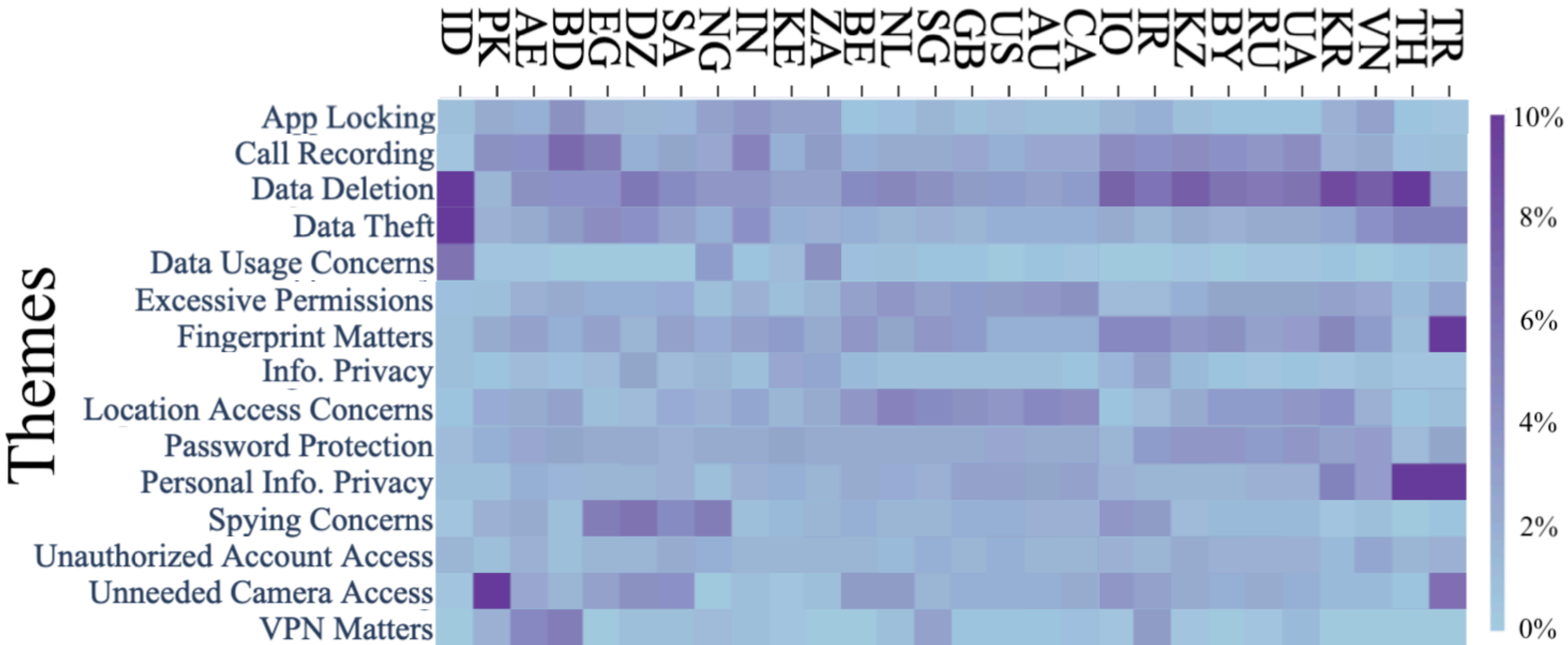
Access to financial services is crucial for economic growth and has been promoted by the United Nations as fundamental in eradicating poverty and achieving the Sustainable Development Goals [1]. However, according to the World Bank [2], about 1.7 billion adults in the world remain unbanked with no access to the services of a bank or similar financial institutions. The largest proportions of unbanked population in developing economies such as Kenya are women, with 50% of the population being unbanked.

Kenya, particularly, has been one of the developing countries that has seen the earliest and perhaps most widespread adoption and usage of mobile loan applications. This has been fueled by the country’s huge success of mobile money services such as M-Pesa [4], [9] coupled with growing smartphone adoption [10] that allows users to apply and receive loans from mobile loan applications directly to their mobile phones. Some of the most widely used mobile loan applications such as Tala and Branch began operations in Kenya before diversifying to other developing countries such as India [6].

As this is a relatively new and therefore unregulated industry, mobile loan applications charge extremely high interest rates and often require repayment within shorter durations of time, compared to traditional financial institutions such as banks. Further, they collect significant sensitive data from users via data available on the mobile device, authorized through the phone’s permission system. This includes collection of contacts and location as part of verifying and calculating users’ credit worthiness [8], [9]. Tala, for example, claims to have repayment rates of more than 90% achieved through modelling users’ routine habits by tracking places they regularly visit, people they frequently contact etc [8].

Despite widely reported privacy concerns [11]–[13], most mobile loan applications claim that users have no concerns, with Shivani Siroya, the founder of Tala, saying “customers have no privacy concerns with Tala as they willingly grant access to their private data through the phone permissions for their credit scores to be developed [8].” Nevertheless, the usage, concerns and behavior with mobile loan applications in the developing world remain largely unexplored.

Countries



Countries

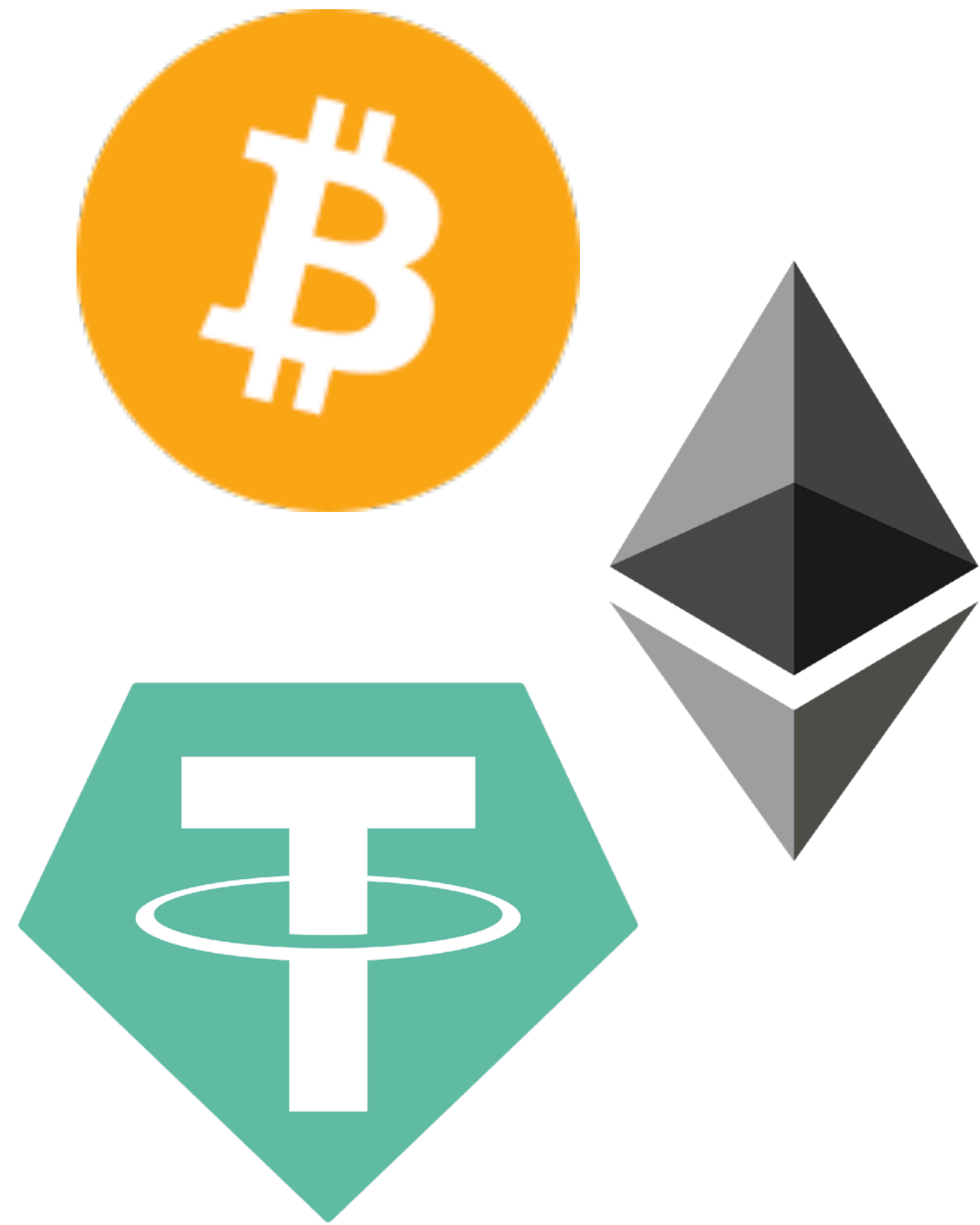
ID PK AE BD EG DZ SA NG IN KE ZA BE NI SG GB AD CA IO IR KZ BY RU UA KR VN TH TR

Themes

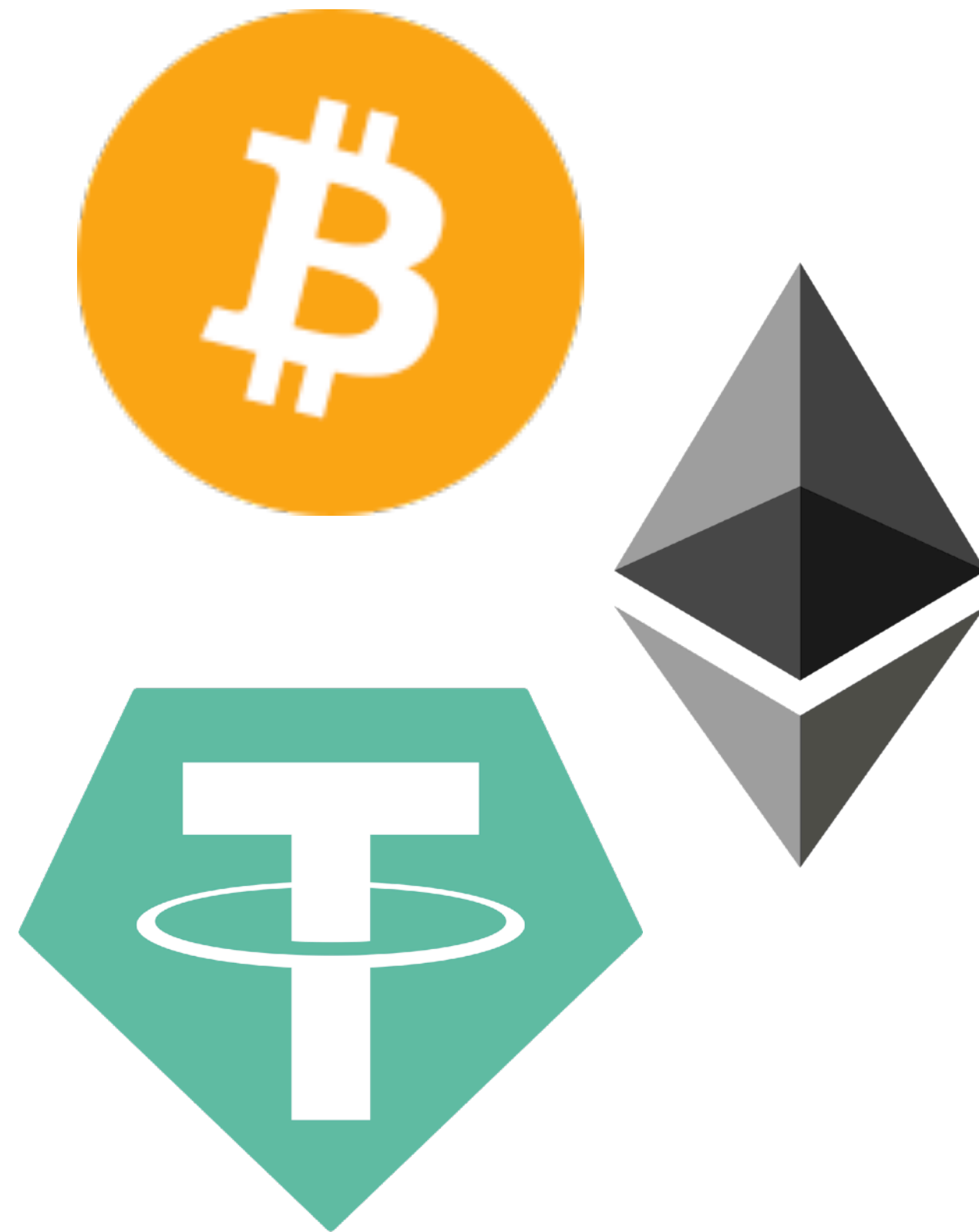


Reviews: legal notice?

Reviews: legal notice?

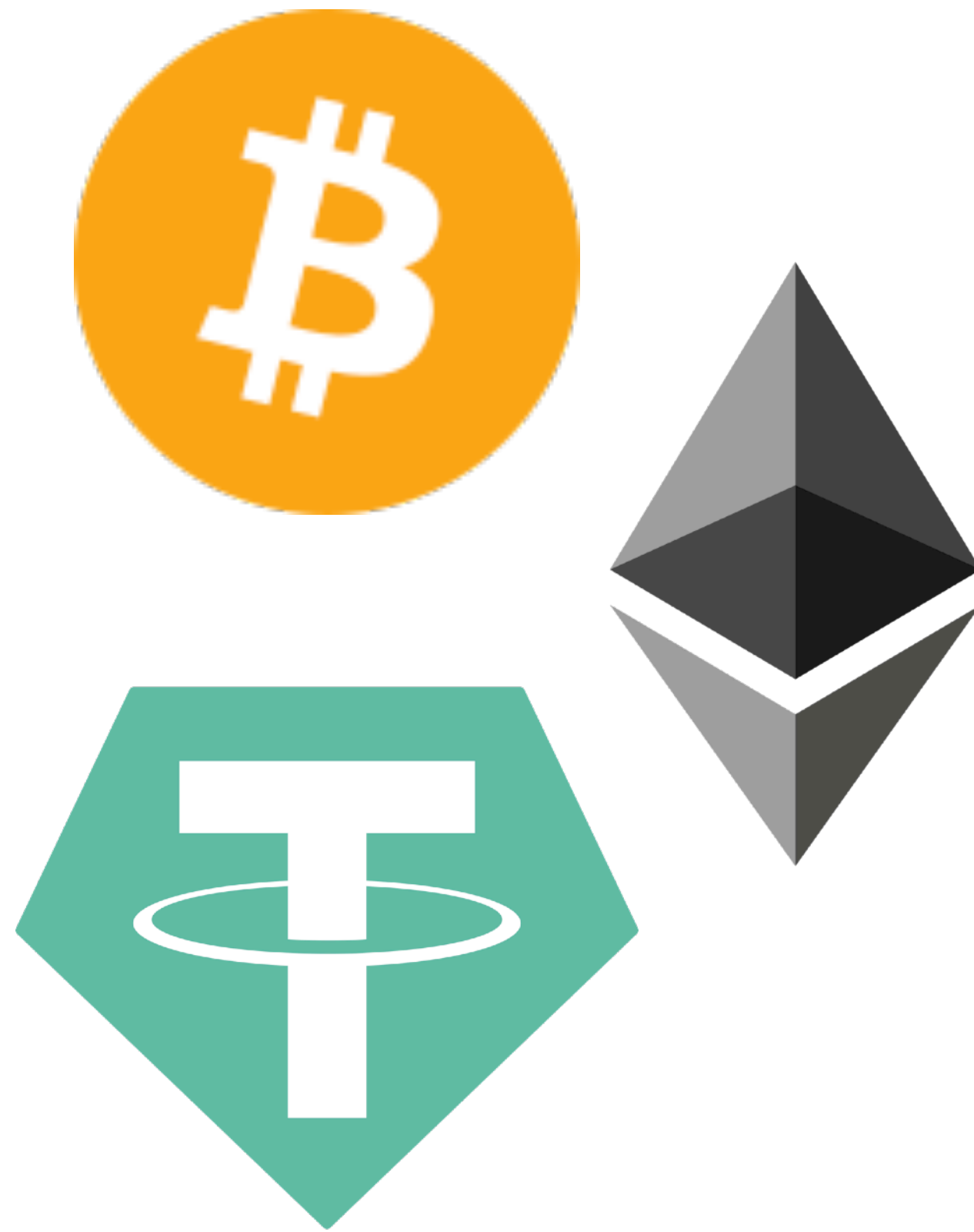


Reviews: legal notice?



A screenshot of the Google Play Store interface. At the top, the 'Google Play' logo is visible along with search, help, and profile icons. The main content area features the app 'Buy Bitcoin & Crypto' with a teal square icon. Below the app name is a white box with a shield icon containing an 'i', containing the text: 'The developer has provided this information about how this app collects, shares, and handles your data'. At the bottom of the screenshot, the 'Data safety' section is partially visible, with the text: 'Here's more information the developer has provided about the kinds of data this app may collect and share, and security practices the app may follow. Data practices may vary based on...'. The bottom navigation bar shows icons for Games, Apps (highlighted), Movies & TV, Books, and Kids.

Reviews: legal notice?



Google Play

collect and share your data. Data privacy and security practices may vary based on your use, region, and age. The developer provided this information and may update it over time.

- This app may share these data types with third parties
Location, Personal info and 7 others
- This app may collect these data types
Location, Personal info and 9 others
- Data is encrypted in transit
- You can request that data be deleted

[See details](#)

Ratings and reviews →

Ratings and reviews are verified ⓘ

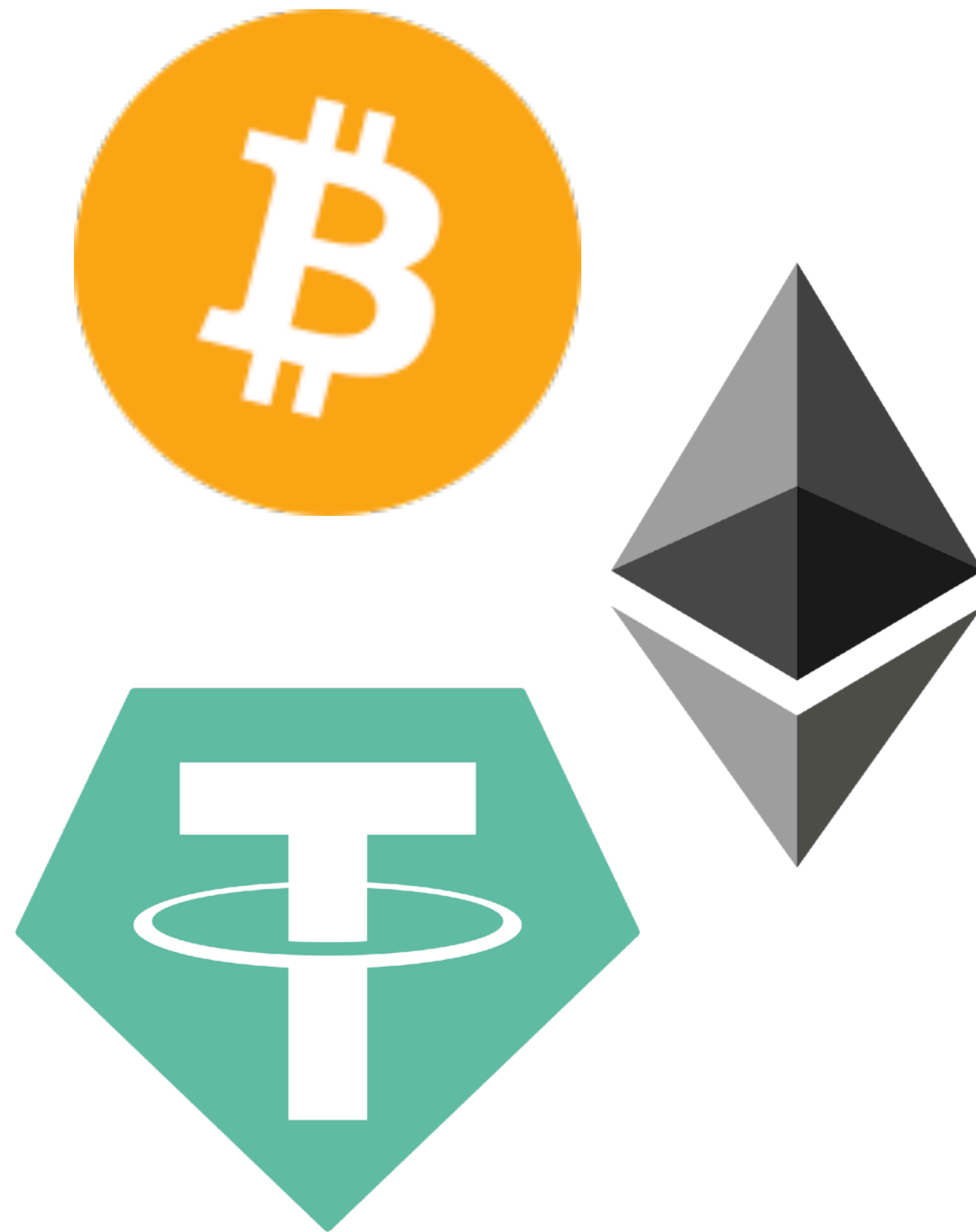
Phone Chromebook Tablet

4.4

5
4
3
2

Games Apps Movies &... Books Kids

Reviews: legal notice?



Google Play

collect and share your data. Data privacy and security practices may vary based on your use, region, and age. The developer provided this information and may update it over time.

- This app may share these data types with third parties
Location, Personal info and 7 others
- This app may collect these data types
Location, Personal info and 9 others
- Data is encrypted in transit
- You can request that data be deleted

[See details](#)

Ratings and reviews →

Ratings and reviews are verified ⓘ

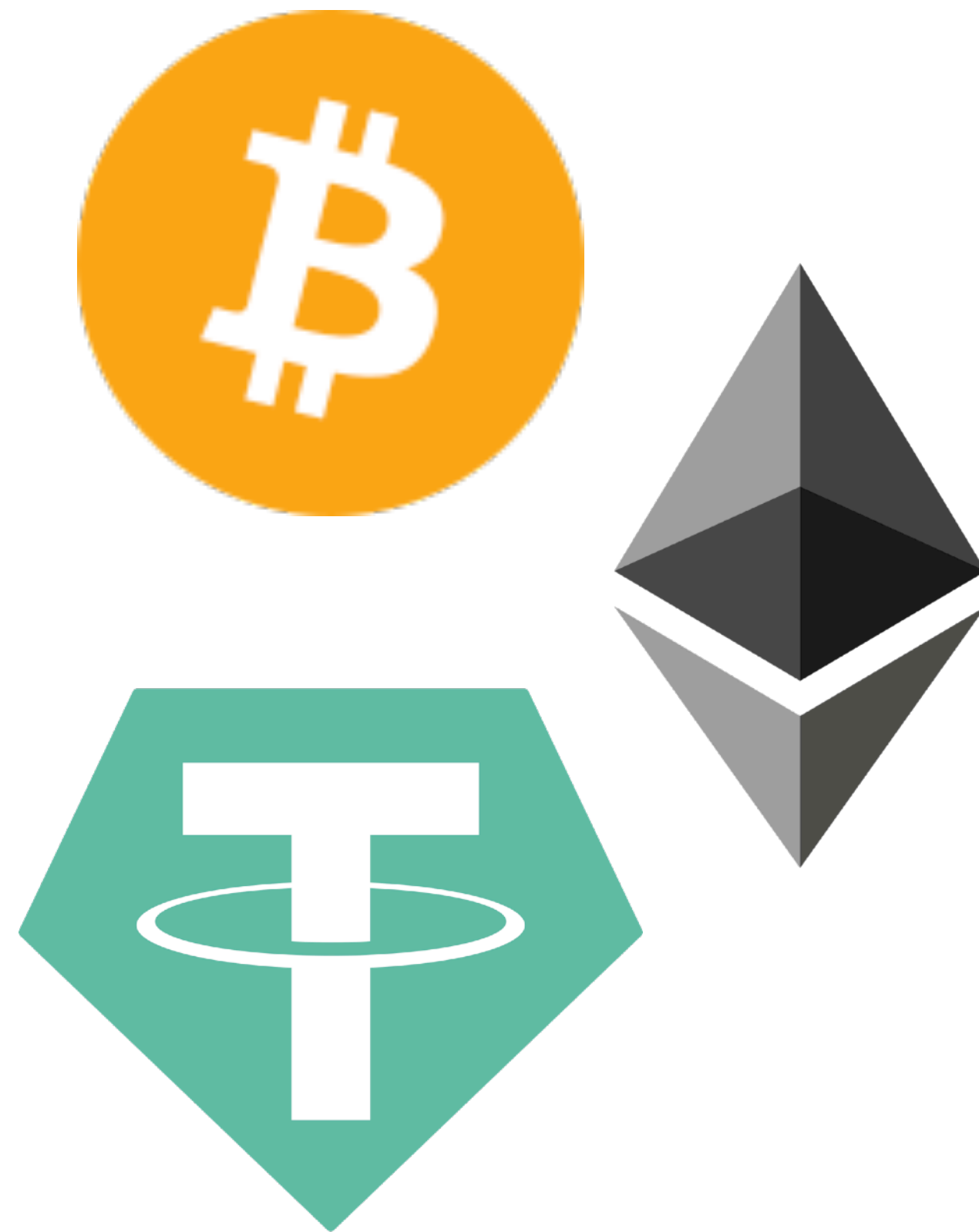
Phone Chromebook Tablet

4.4

5
4
3
2

Games Apps Movies &... Books Kids

Reviews: legal notice?



A screenshot of the Google Play Store page for an app titled "Coin: Buy...". The page shows data privacy information, including data types shared with third parties (Location, Personal info, and 7 others), data types collected (Location, Personal info, and 9 others), and a note that data is encrypted in transit. Below this, the "Ratings and reviews" section is highlighted with a red box. The rating is 4.4, and the page shows a bar chart for the rating distribution. The bottom navigation bar includes icons for Games, Apps, Movies & TV, Books, and Kids.

A screenshot of a user review for the app "Coin: Buy...". The review is from a user from Türkiye and contains a legal notice: "I [give] no permission to share things (My photo, national ID number, password, etc.) with third parties. And if such thing happens, the app bears sole responsibility and I will take legal action against them." The review is dated April 30, 2021, and has a 4-star rating. Below the review, there are buttons for "Yes" and "No" to indicate if the review was helpful. The bottom of the screenshot shows the app's navigation bar.

Reviews: legal notice?

Reviews: legal notice?

- Large amount of such reviews from Türkiye 

Reviews: legal notice?

- Large amount of such reviews from Türkiye 🇹🇷



Reviews: legal notice?

- Large amount of such reviews from Türkiye 🇹🇷
- Unclear: they believe it's protective



Reviews: legal notice?

- Large amount of such reviews from Türkiye 🇹🇷
- Unclear: they believe it's protective
- Indicative: they care

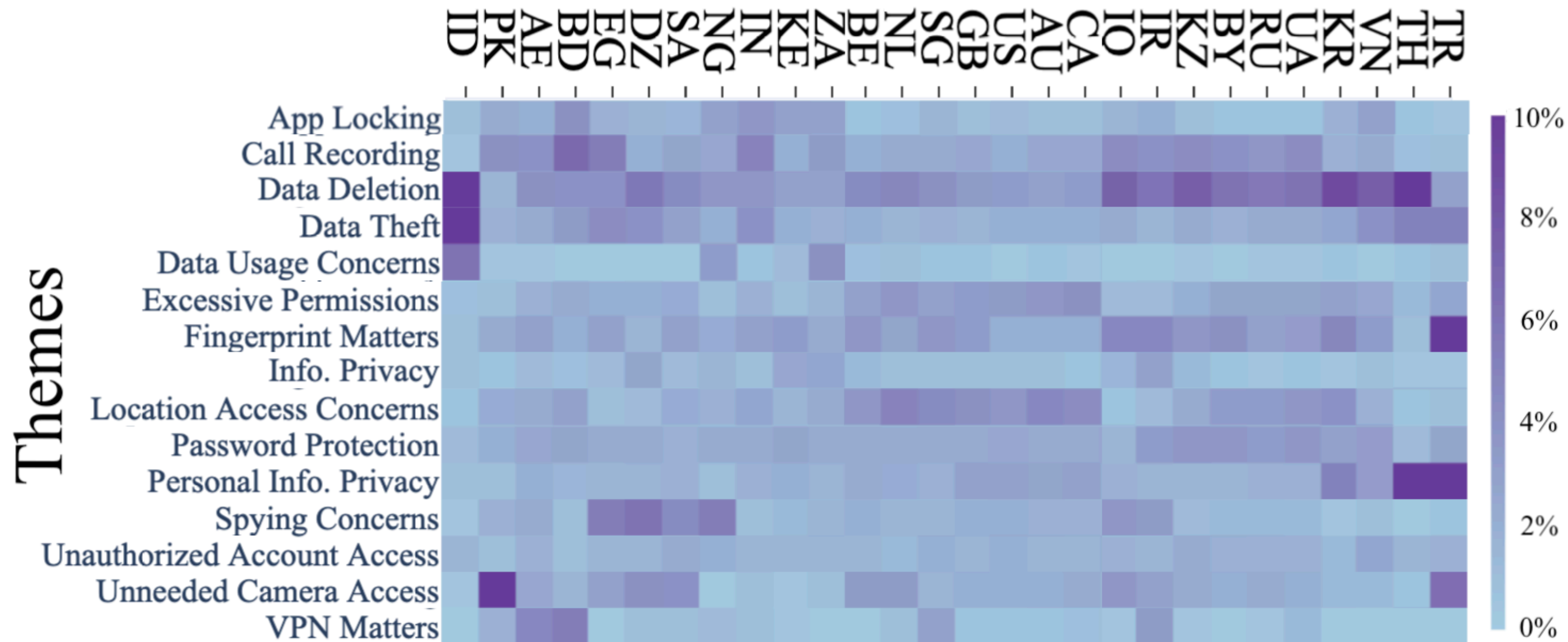


Reviews: legal notice?

- Large amount of such reviews from Türkiye 🇹🇷
- Unclear: they believe it's protective
- Indicative: they care
- We need research to know



Countries



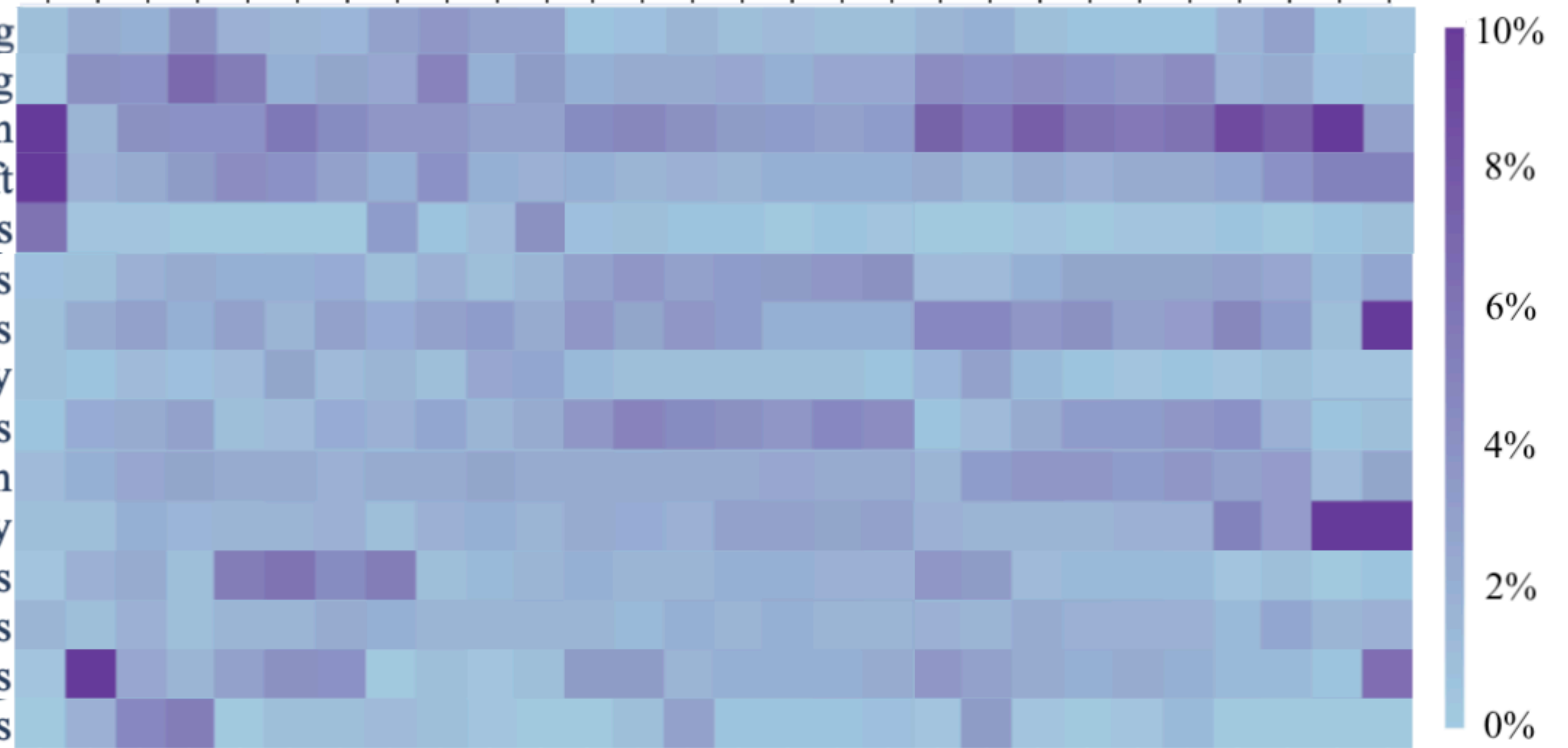


Countries

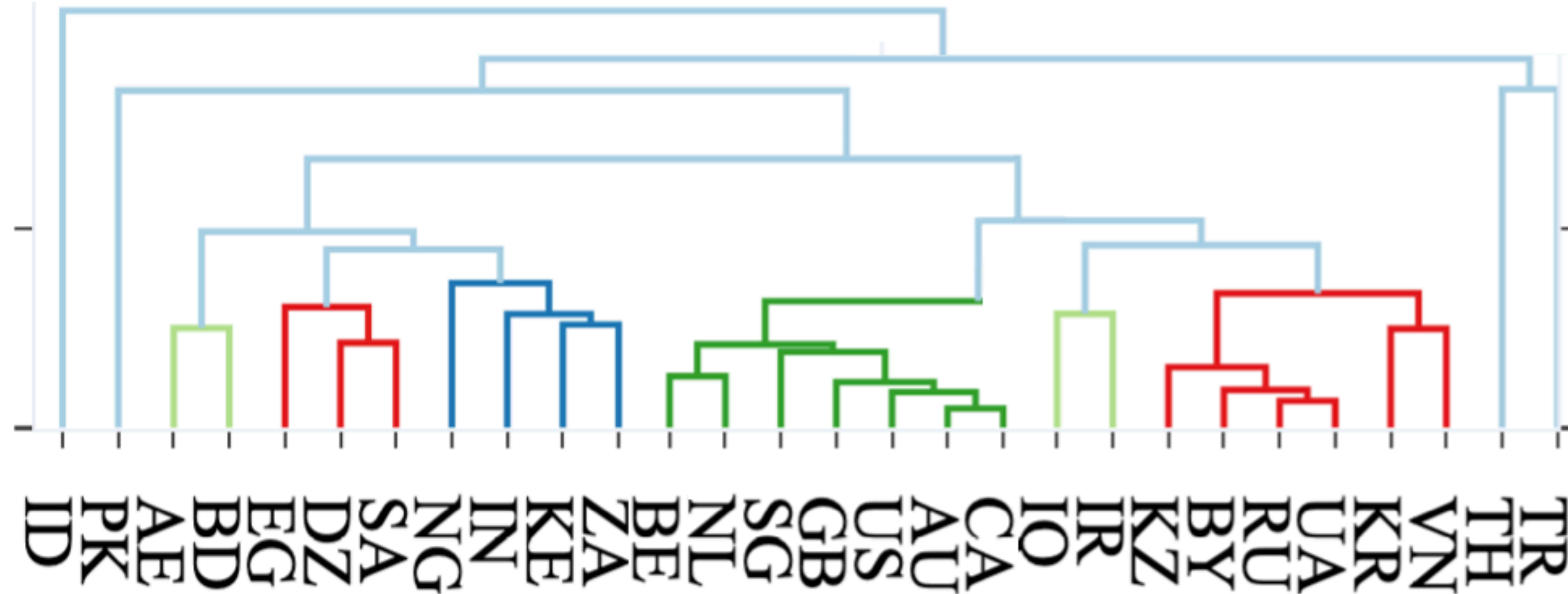
Themes

- App Locking
- Call Recording
- Data Deletion
- Data Theft
- Data Usage Concerns
- Excessive Permissions
- Fingerprint Matters
- Info. Privacy
- Location Access Concerns
- Password Protection
- Personal Info. Privacy
- Spying Concerns
- Unauthorized Account Access
- Unneeded Camera Access
- VPN Matters

TR TH VN KR UA RU BY KZ IR IO CA AU US GB SG NI BE NZ KE IN SA DN ZG EG BD AE PK ID

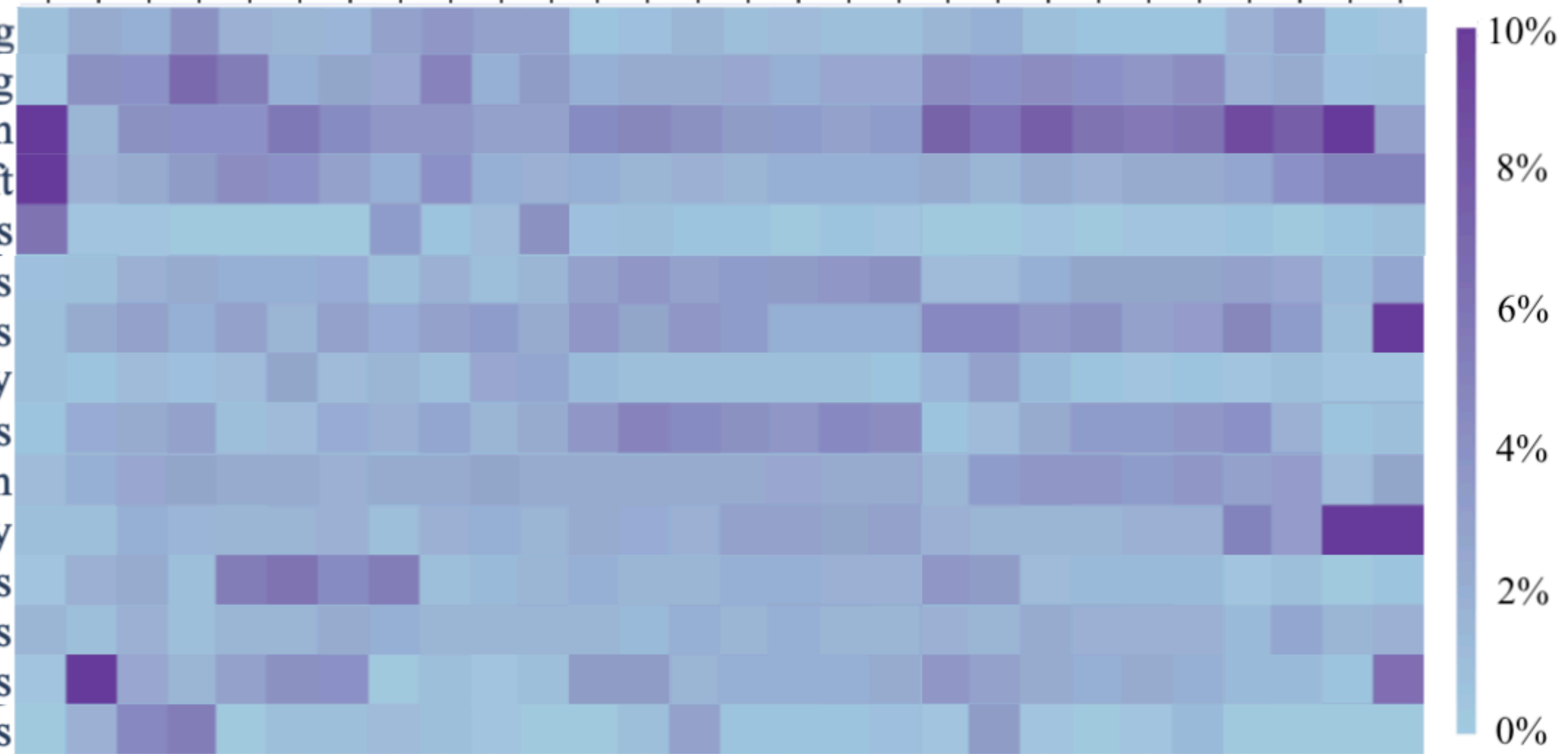


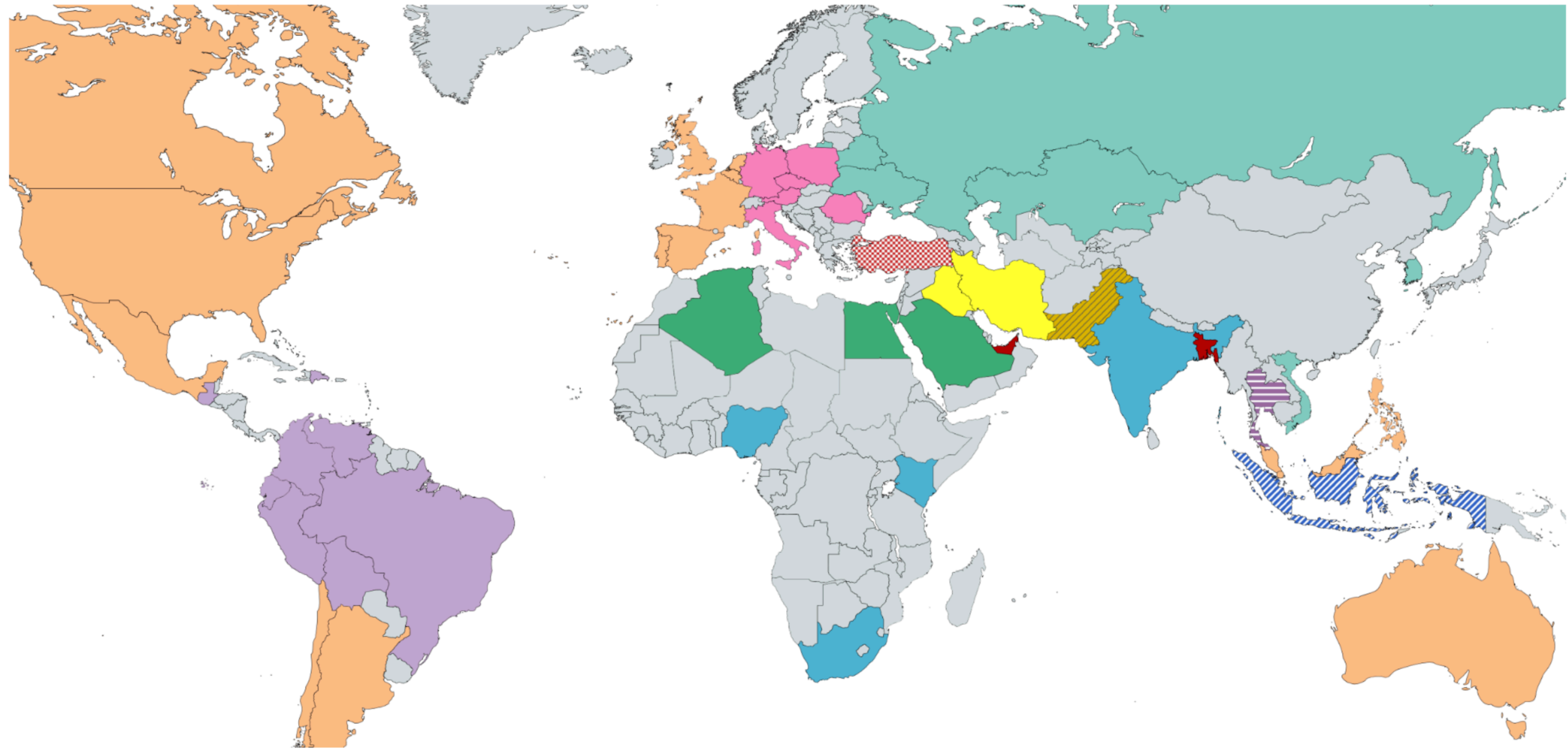
Countries



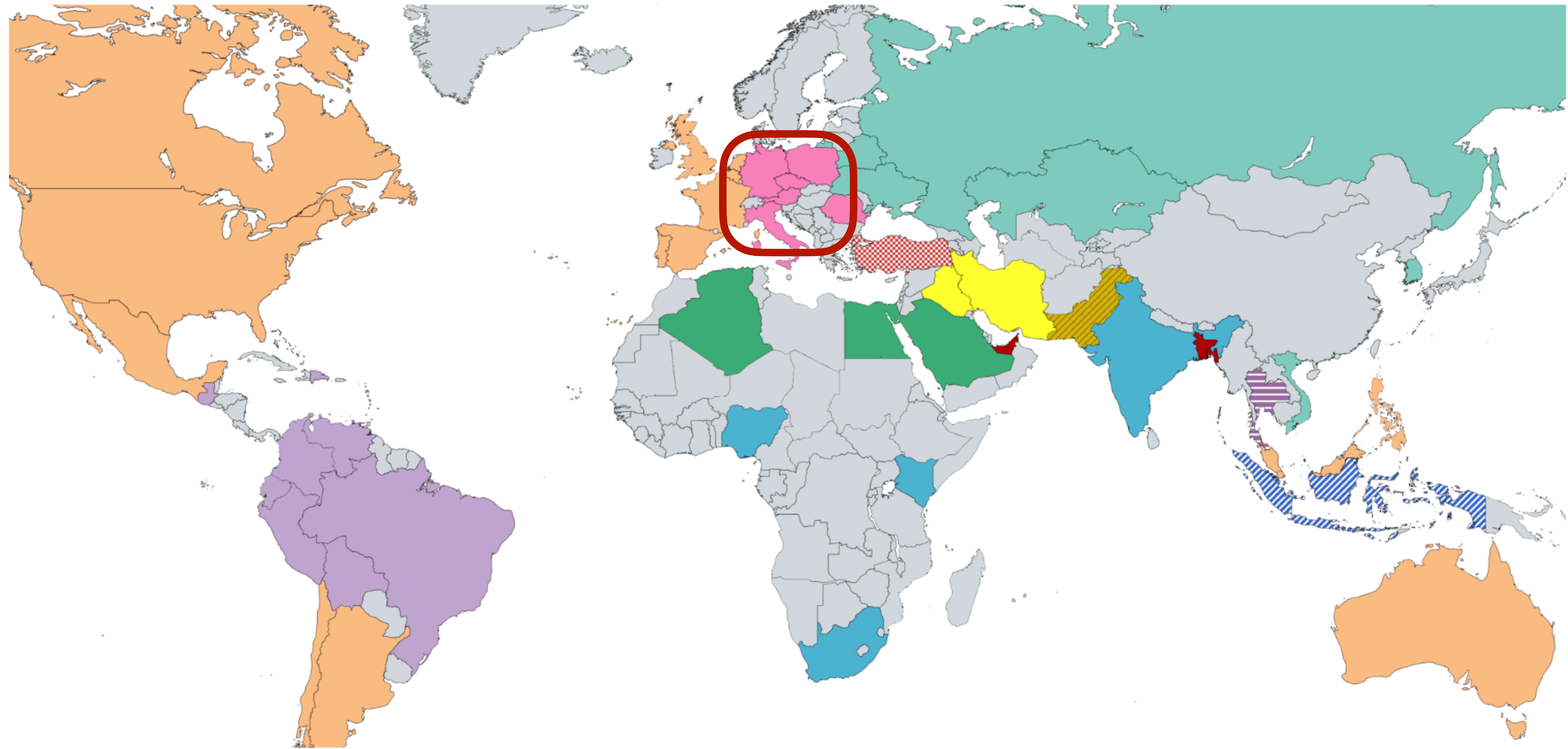
Themes

- App Locking
- Call Recording
- Data Deletion
- Data Theft
- Data Usage Concerns
- Excessive Permissions
- Fingerprint Matters
- Info. Privacy
- Location Access Concerns
- Password Protection
- Personal Info. Privacy
- Spying Concerns
- Unauthorized Account Access
- Unneeded Camera Access
- VPN Matters

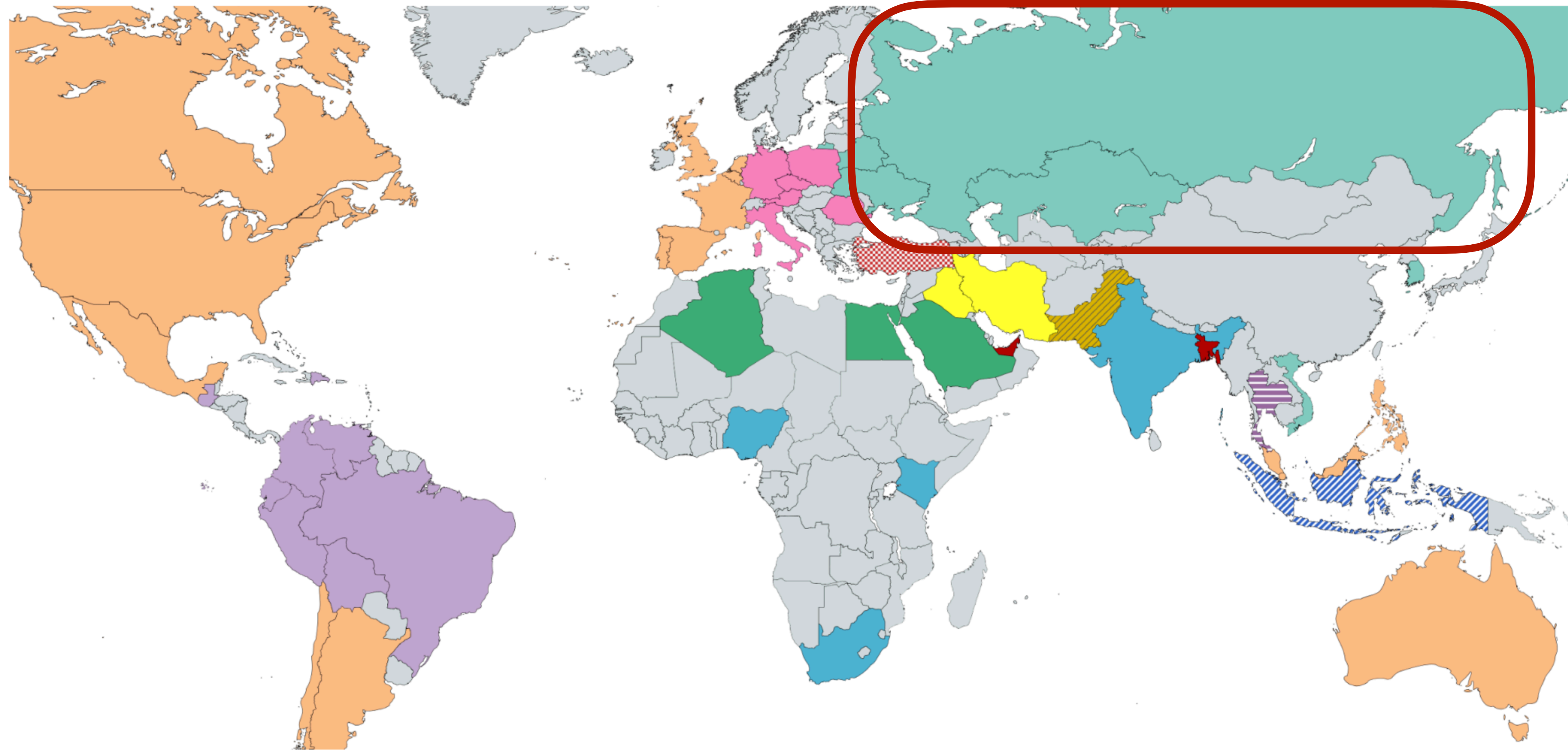




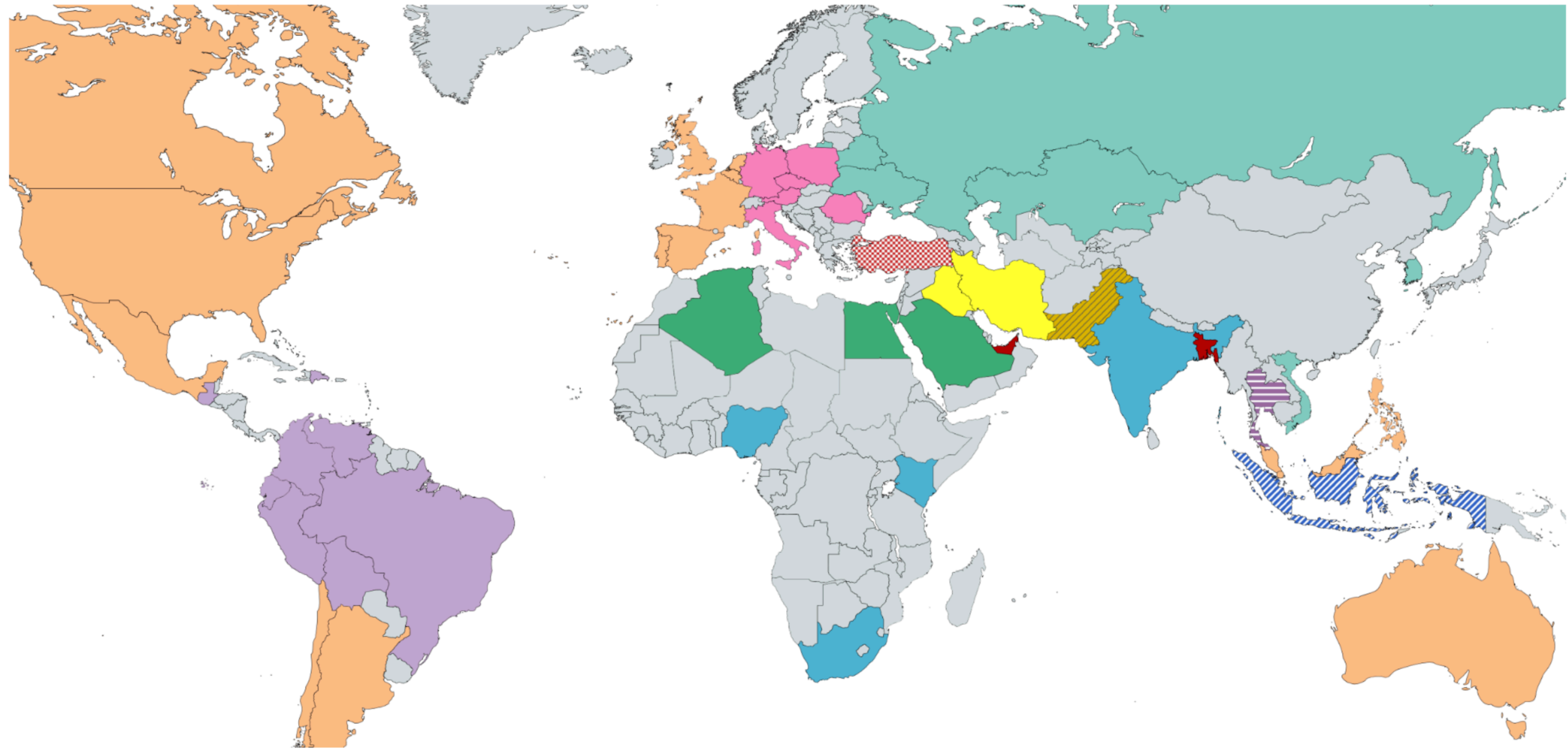
**Similarities between culturally/geographically close countries
this is not a rule!**



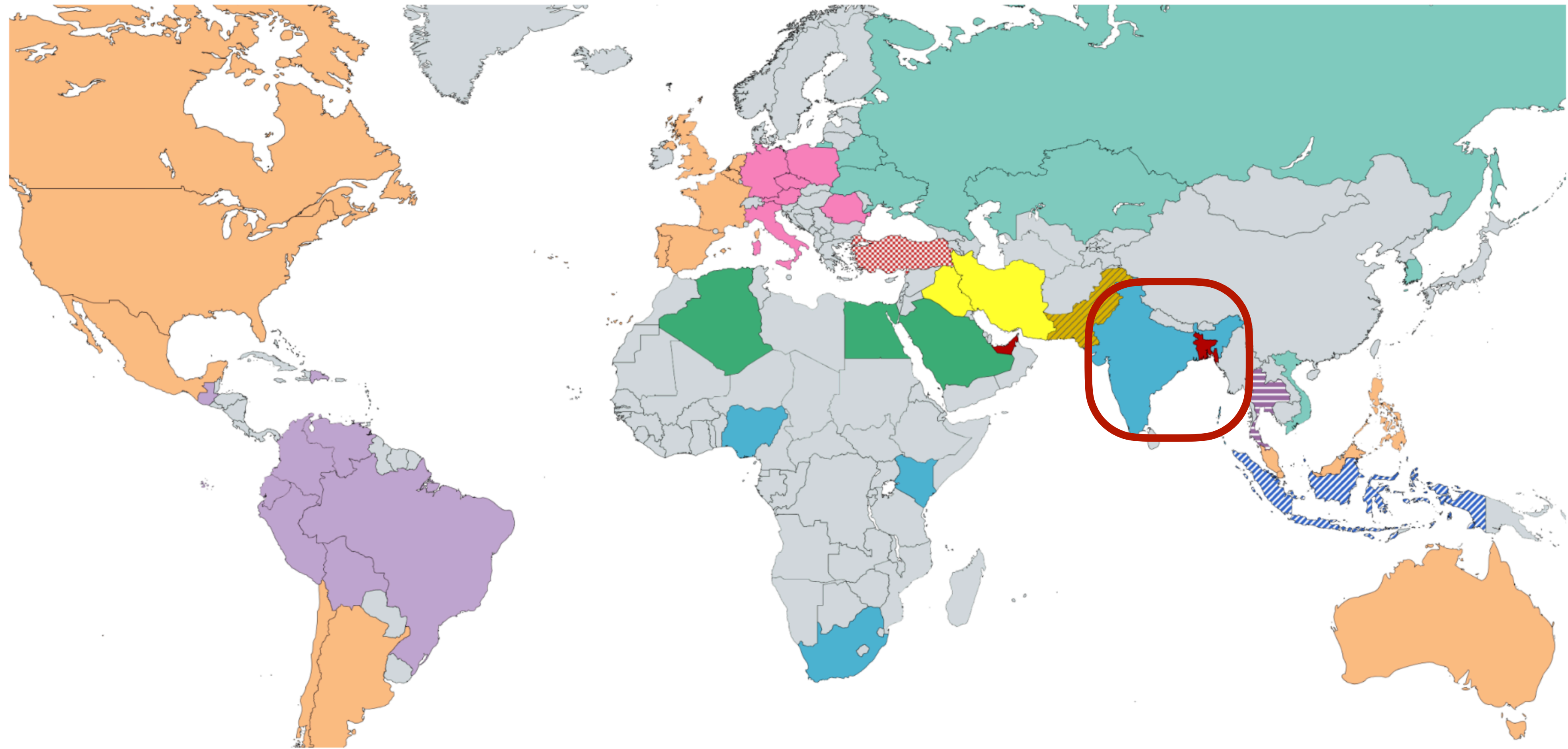
**Similarities between culturally/geographically close countries
this is not a rule!**



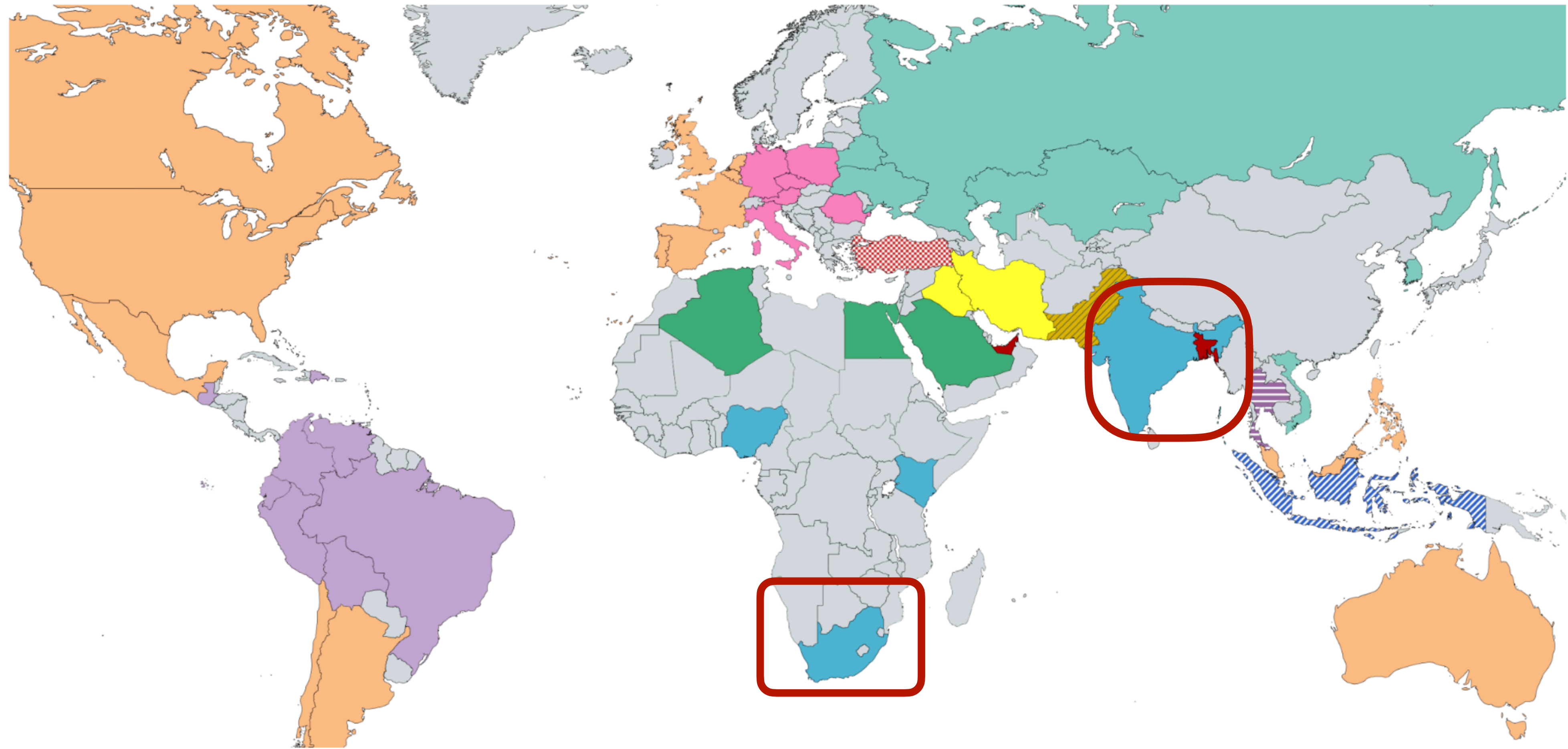
**Similarities between culturally/geographically close countries
this is not a rule!**



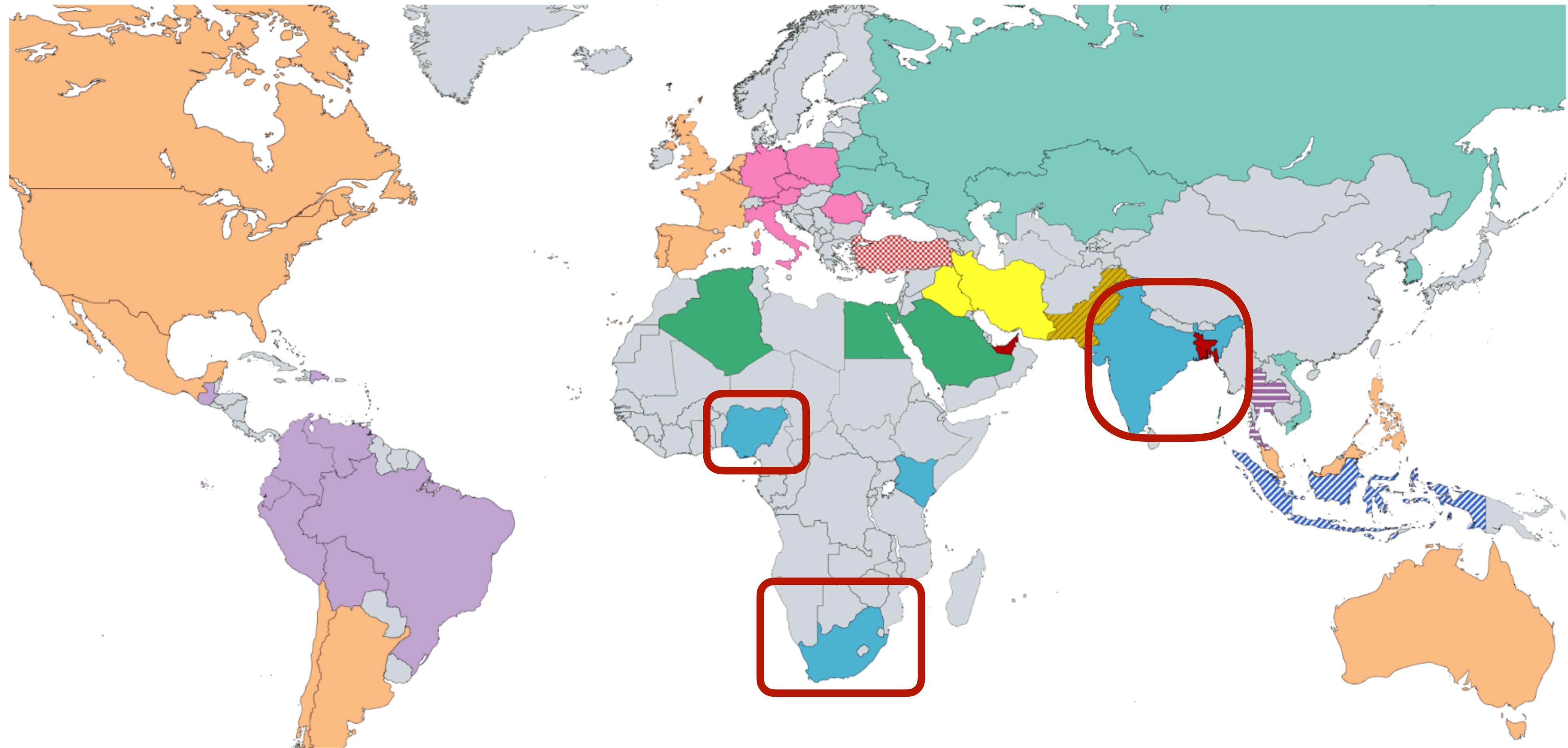
**Similarities between culturally/geographically close countries
this is not a rule!**



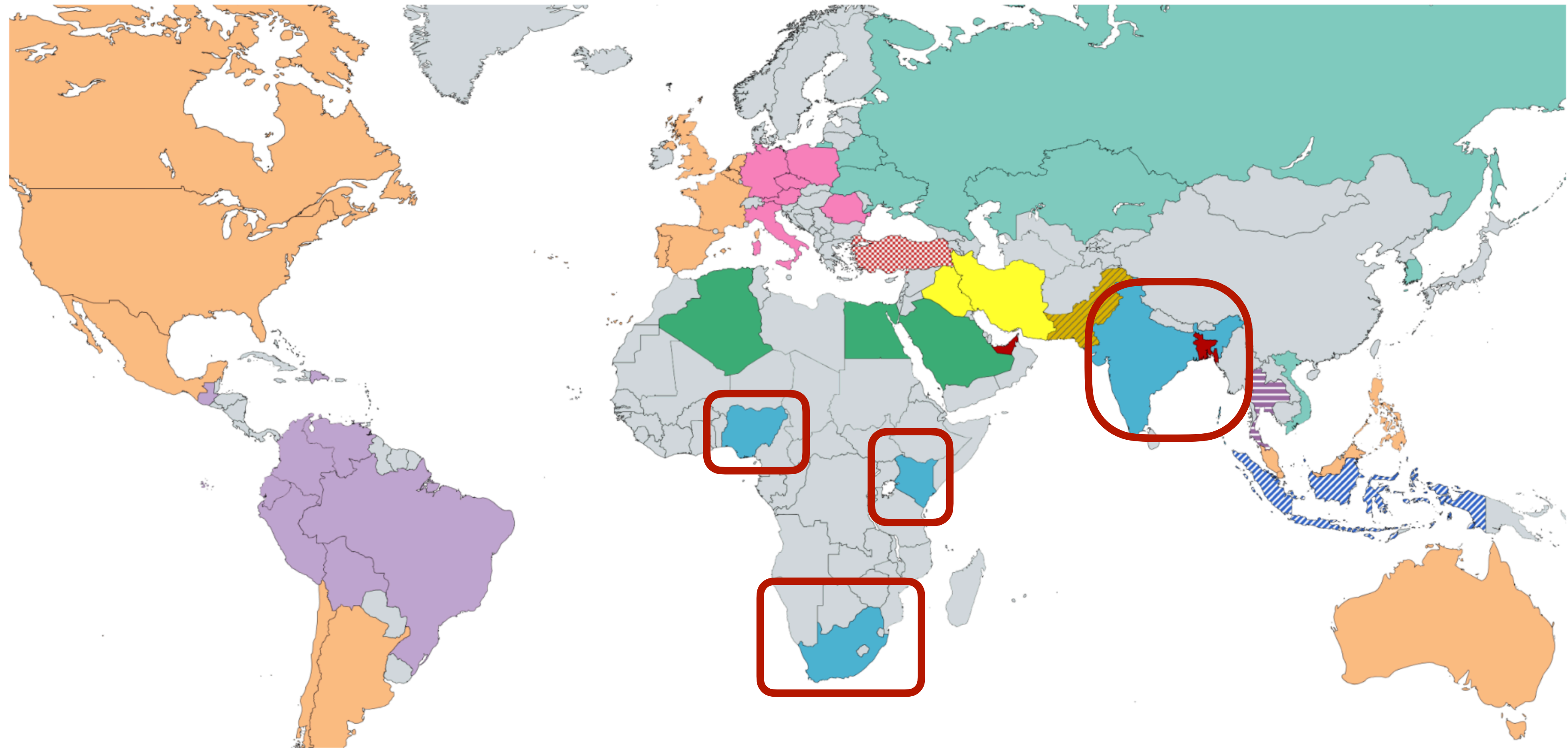
**Similarities between culturally/geographically close countries
this is not a rule!**



**Similarities between culturally/geographically close countries
this is not a rule!**



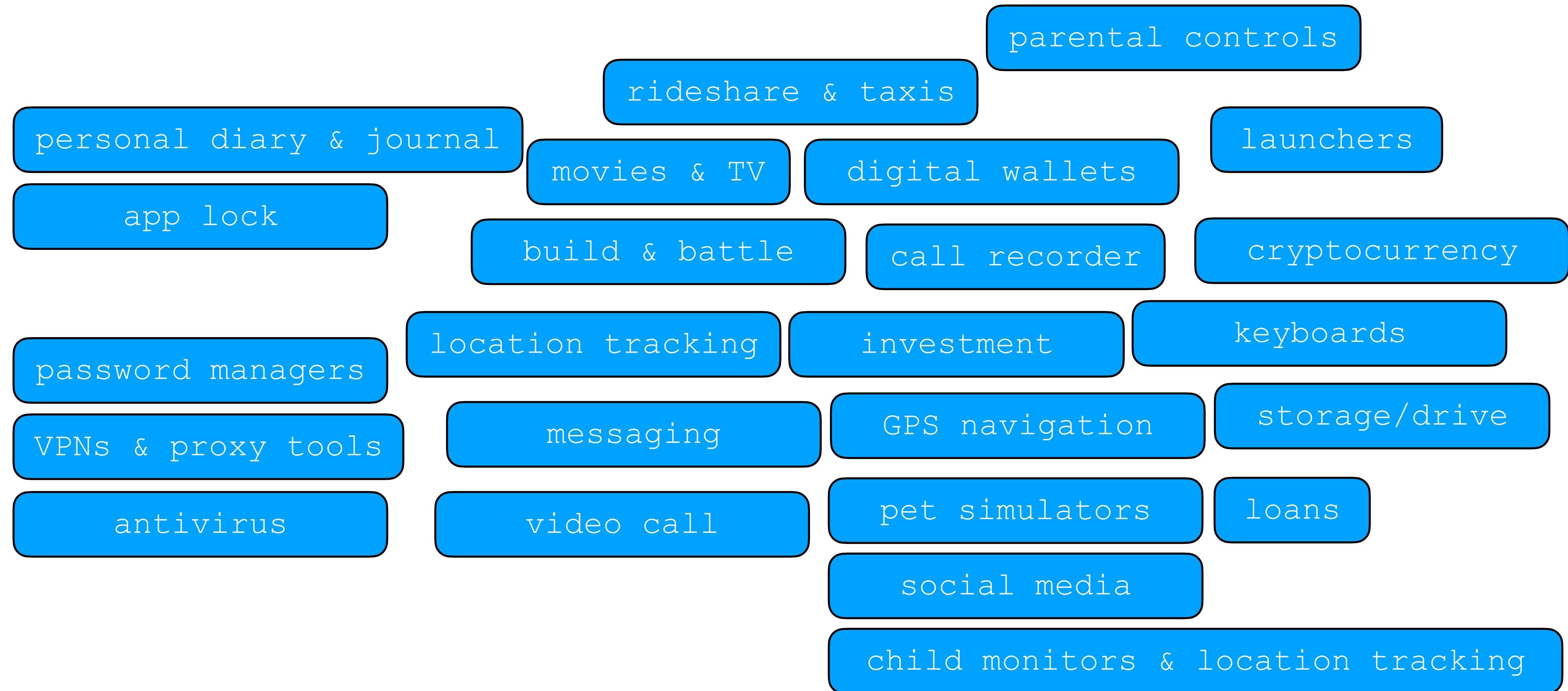
**Similarities between culturally/geographically close countries
this is not a rule!**



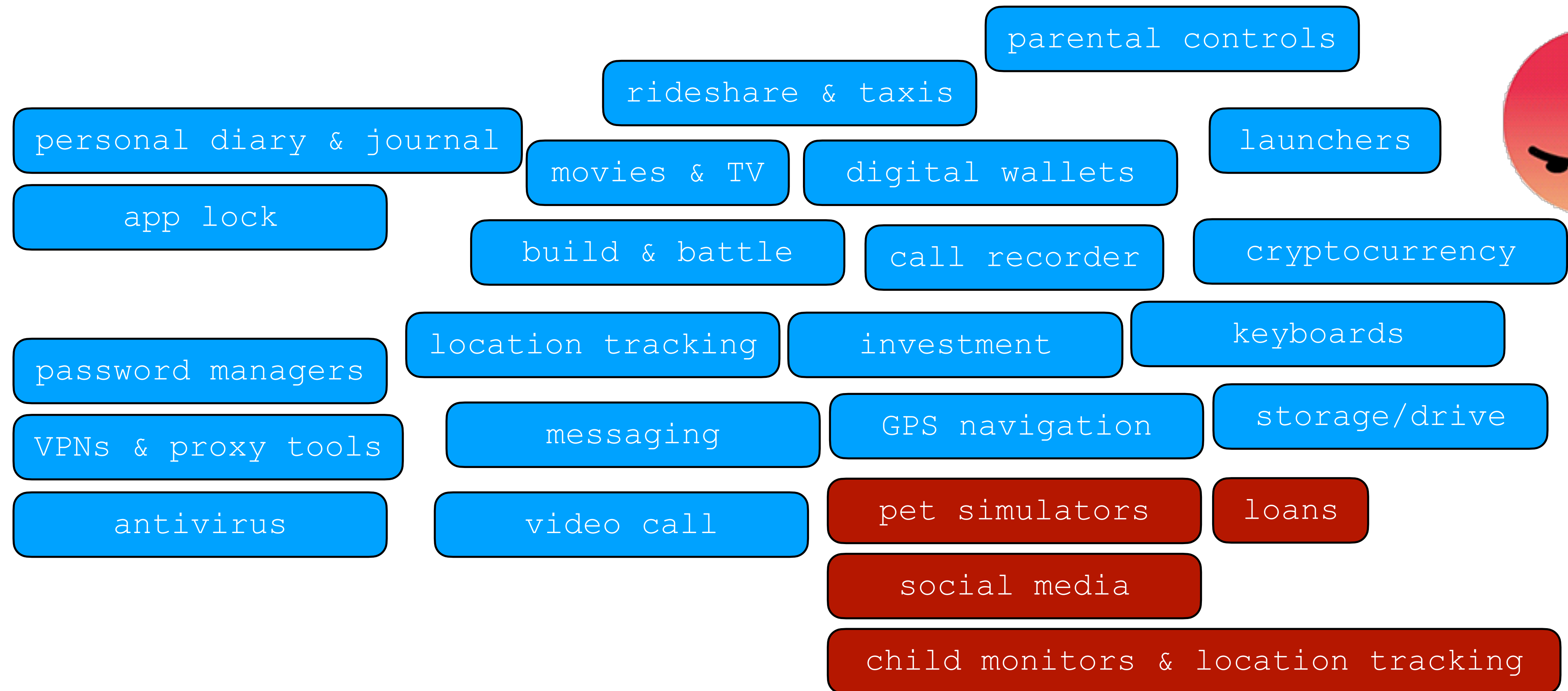
**Similarities between culturally/geographically close countries
this is not a rule!**

What about app types?

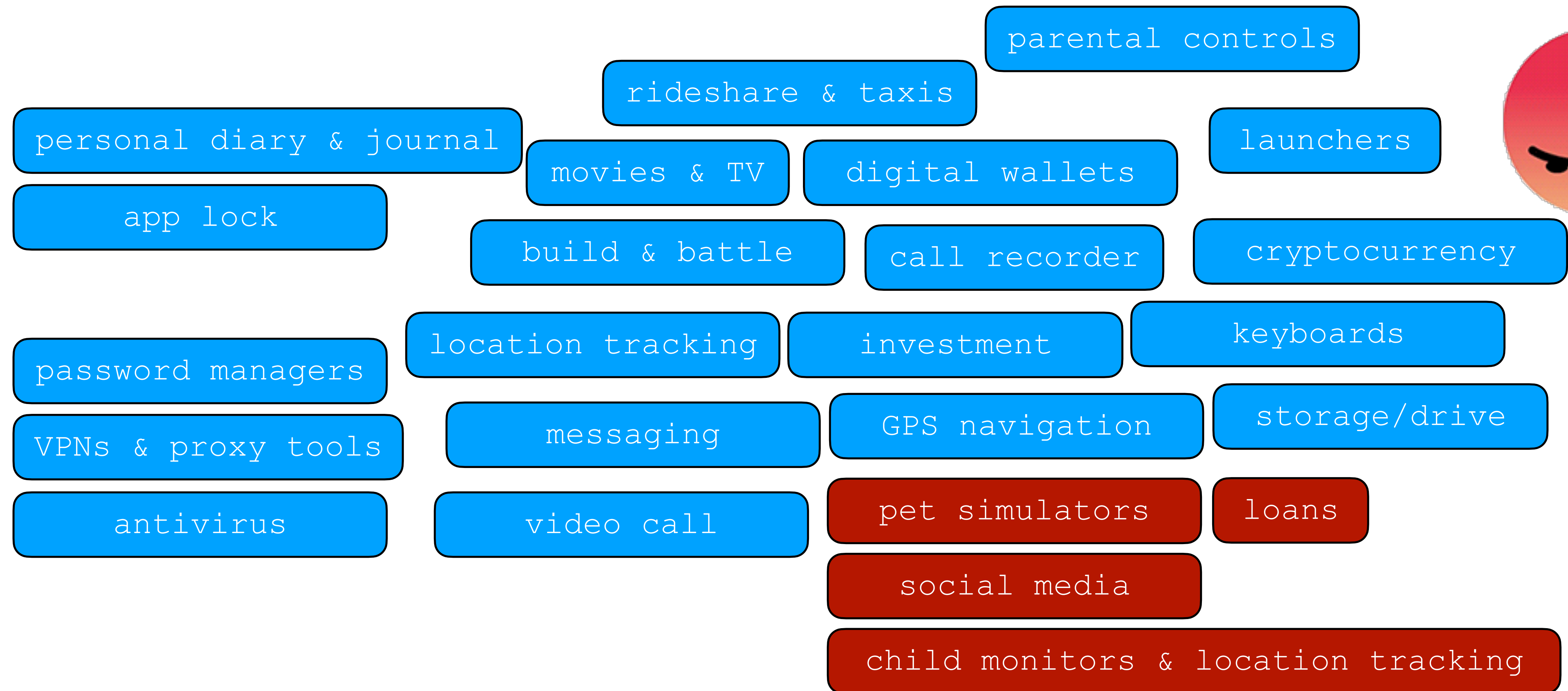
What about app types?



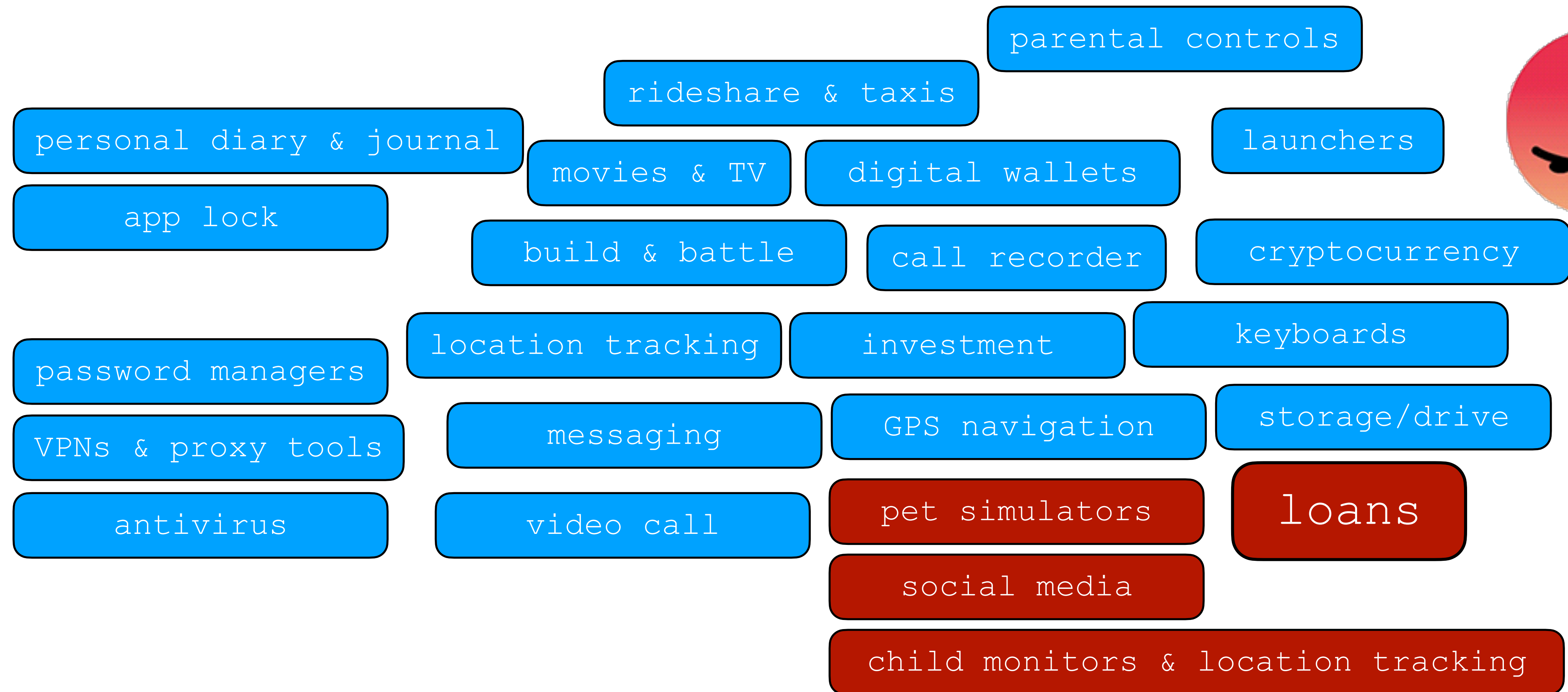
What about app types?



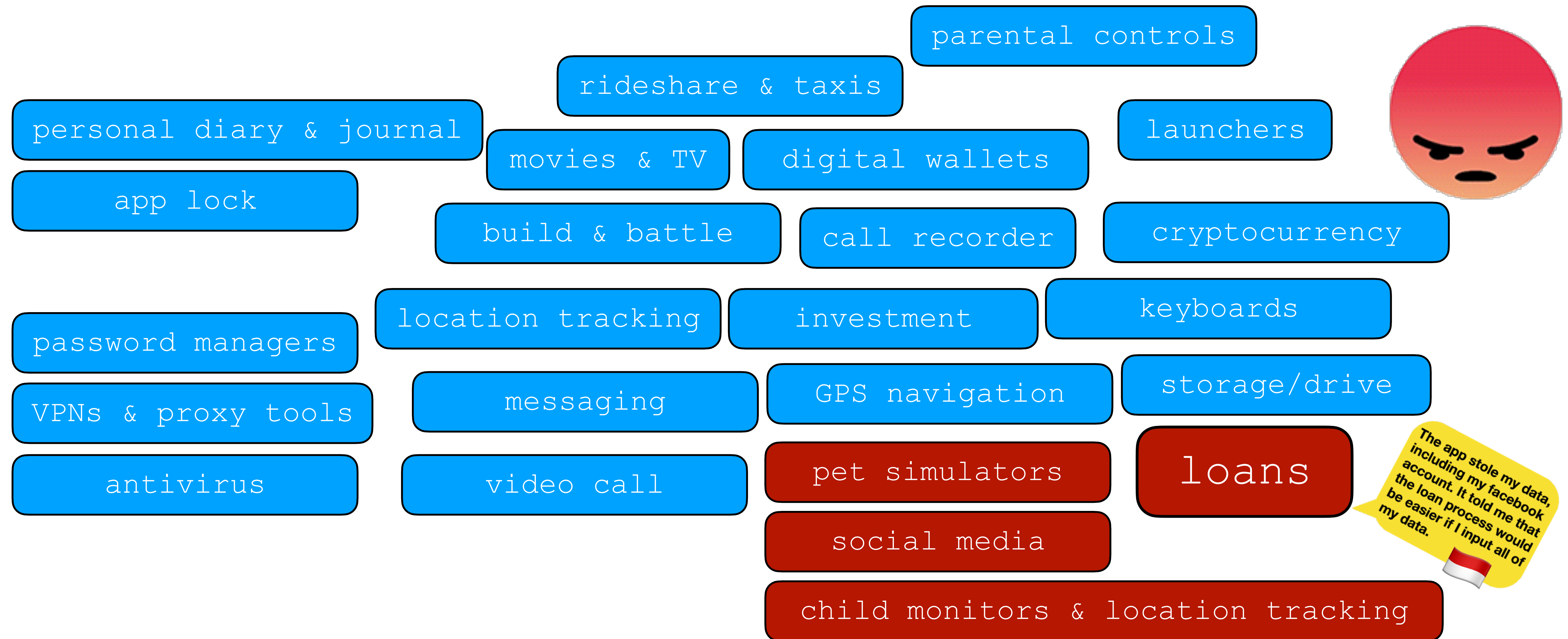
What about app types?



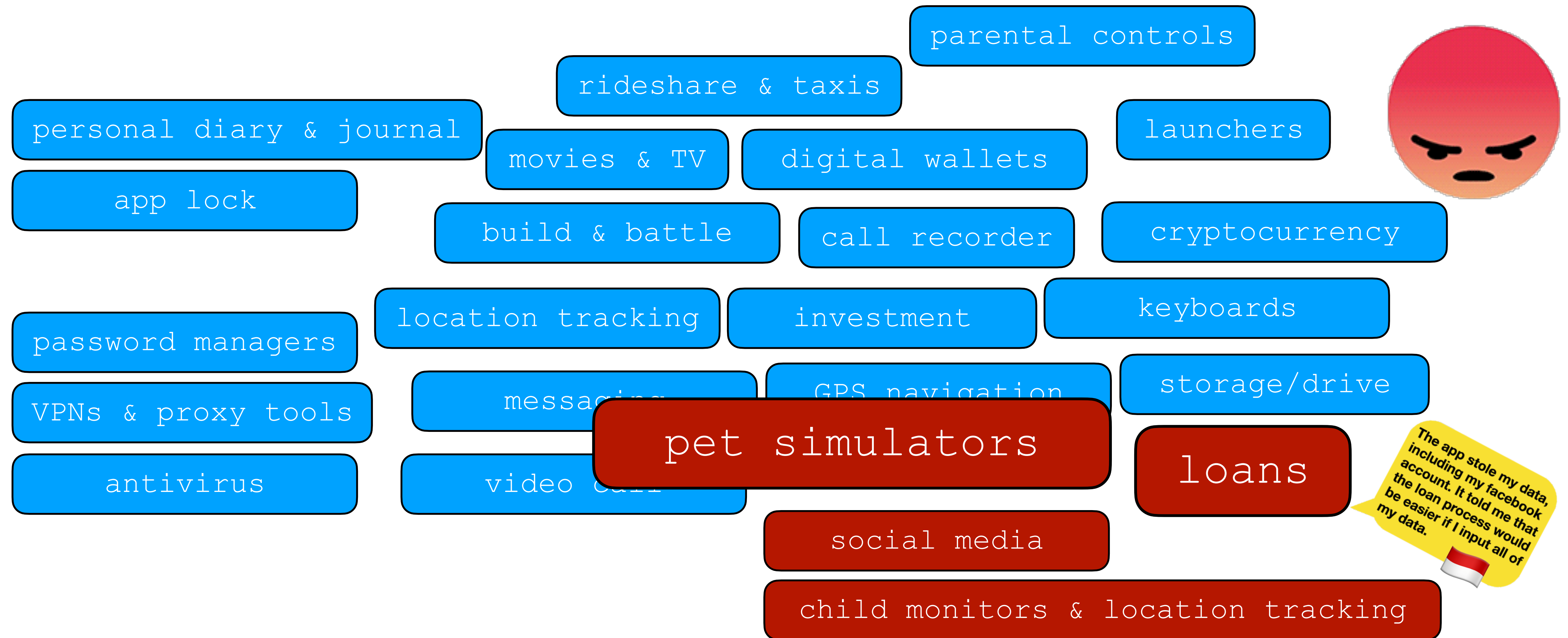
What about app types?



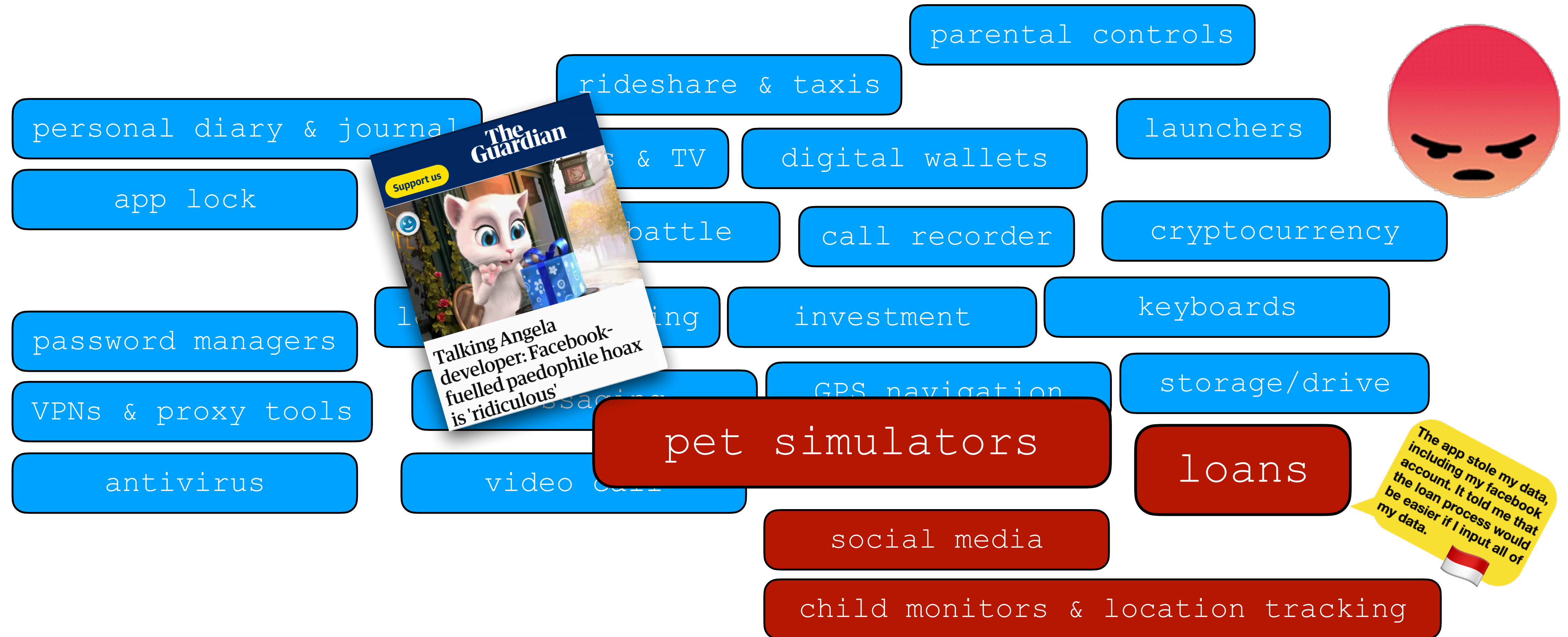
What about app types?



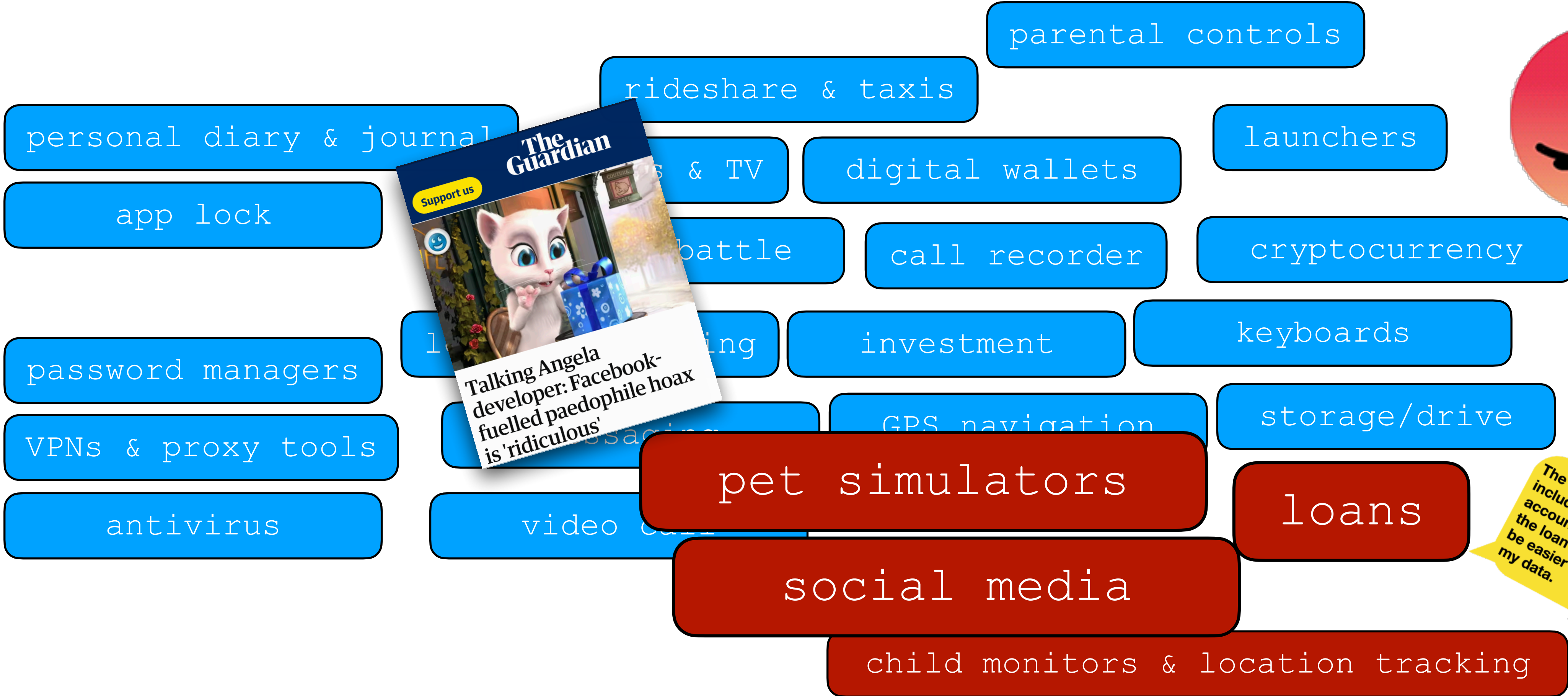
What about app types?



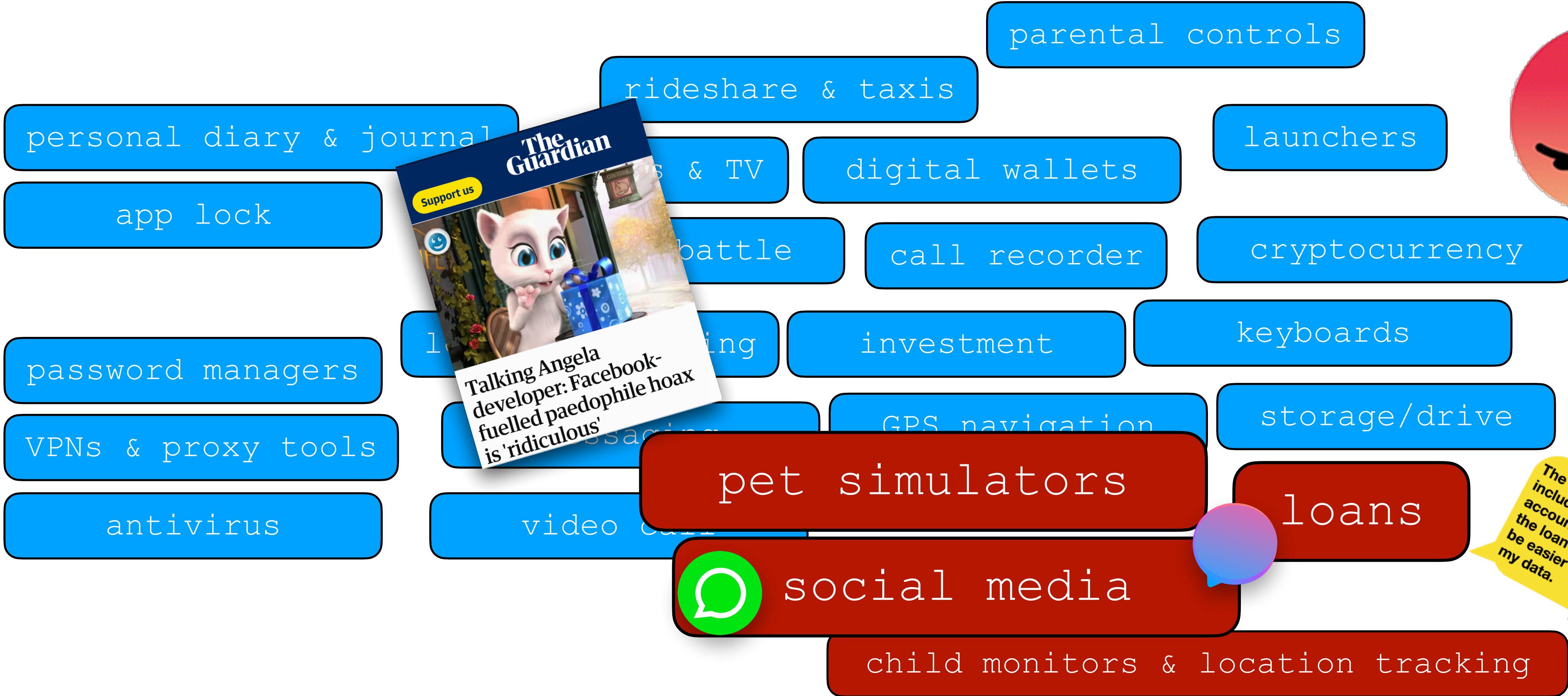
What about app types?



What about app types?



What about app types?



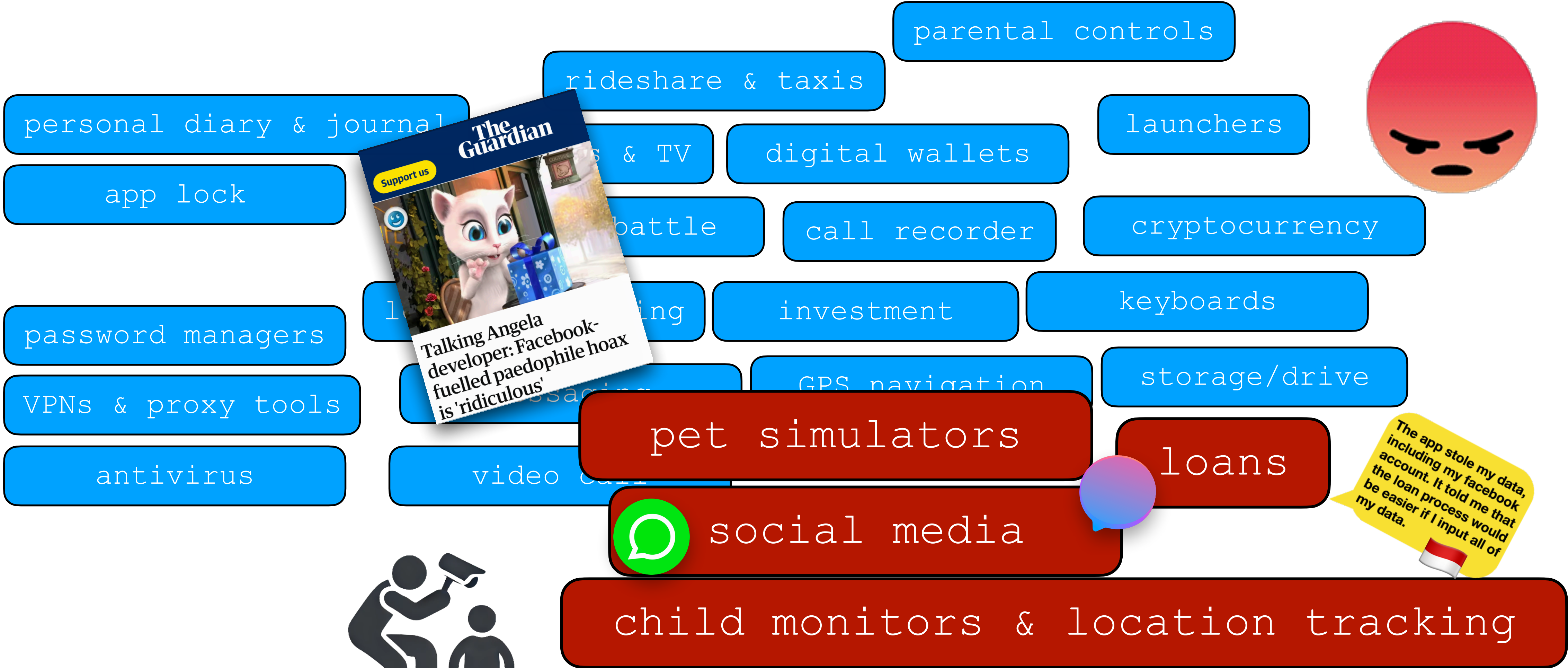
What about app types?



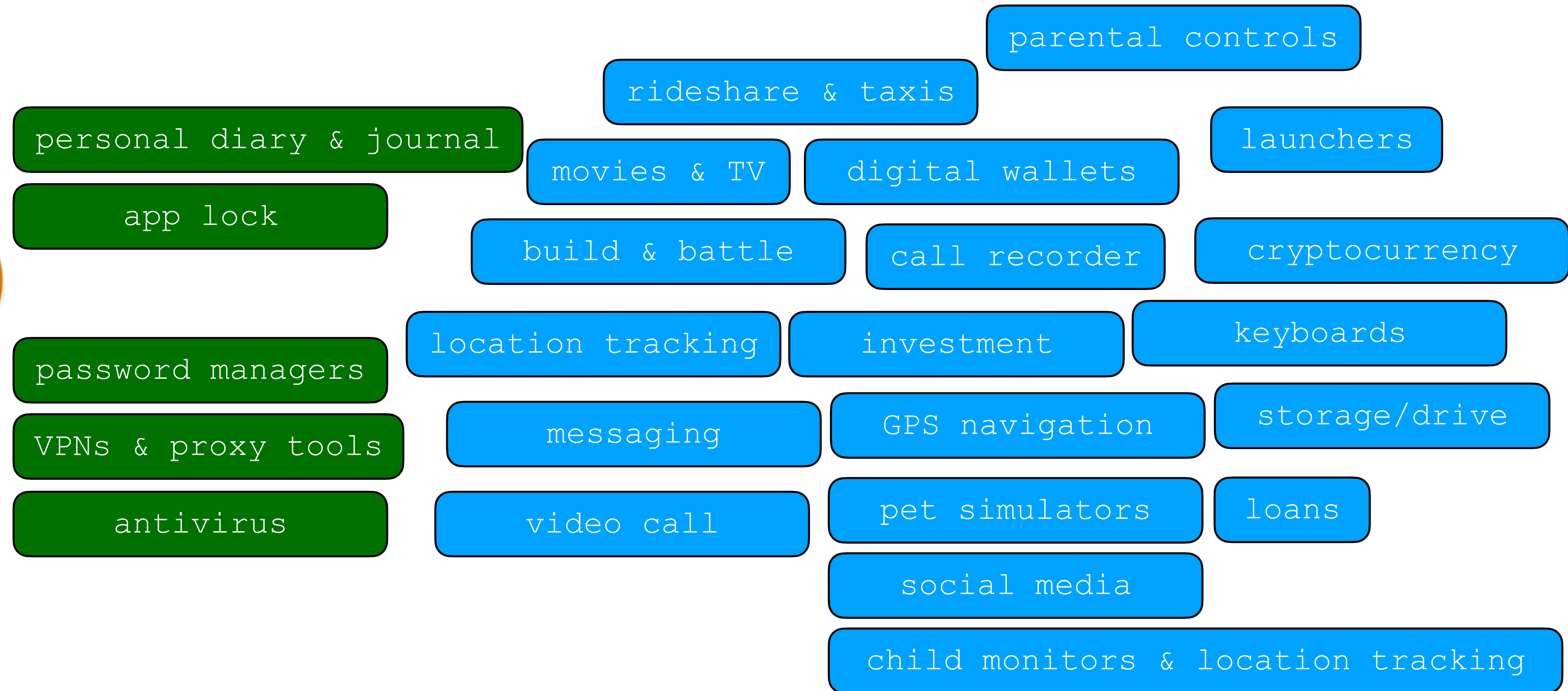
What about app types?



What about app types?



What about app types?



S&P apps, quite positive!



personal diary & journal

app lock

password managers

VPNs & proxy tools

antivirus

S&P apps, quite positive!

personal diary & journal

app lock

password managers

VPNs & proxy tools

antivirus

- People like journaling
- And keeping it secret (with passwords!)



S&P apps, quite positive!

personal diary & journal

app lock

password managers

VPNs & proxy tools

antivirus

- People like journaling

- Hide applications from home screen
- Crucial when sharing device



S&P apps, quite positive!

personal diary & journal

app lock

password managers

VPNs & proxy tools

antivirus

- People like journaling

- Hide applications from home screen
- Crucial when sharing device



S&P apps, quite positive!

personal diary & journal

app lock

password managers

VPNs & proxy tools

antivirus

• People like journaling

• Hide applications from home screen

• Crucial when sharing device



S&P apps, quite positive!

personal diary & journal

- People like journaling

app lock

- Hide applications from

password managers

- Hassle free passwords

- Easy unlock with biometrics

VPNs & proxy tools

antivirus



S&P apps, quite positive!

personal diary & journal

- People like journaling

app lock

- Hide applications from

password managers

- Hassle free passwords

VPNs & proxy tools

- People believe in VPN privacy protections

antivirus

- Reflects what ads say



S&P apps, quite positive!

personal diary & journal

- People like journaling

app lock

- Hide applications from

password managers

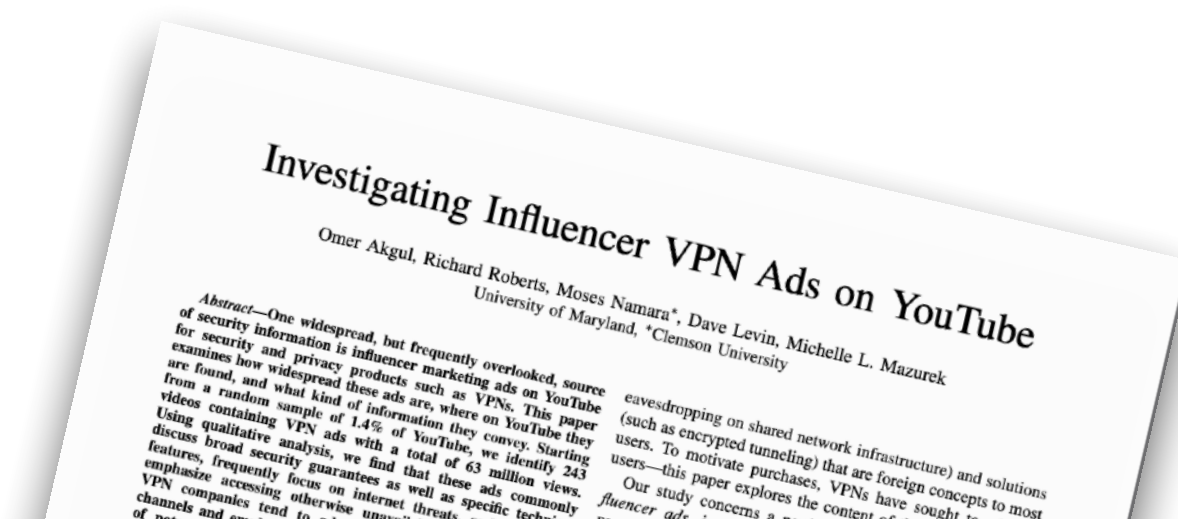
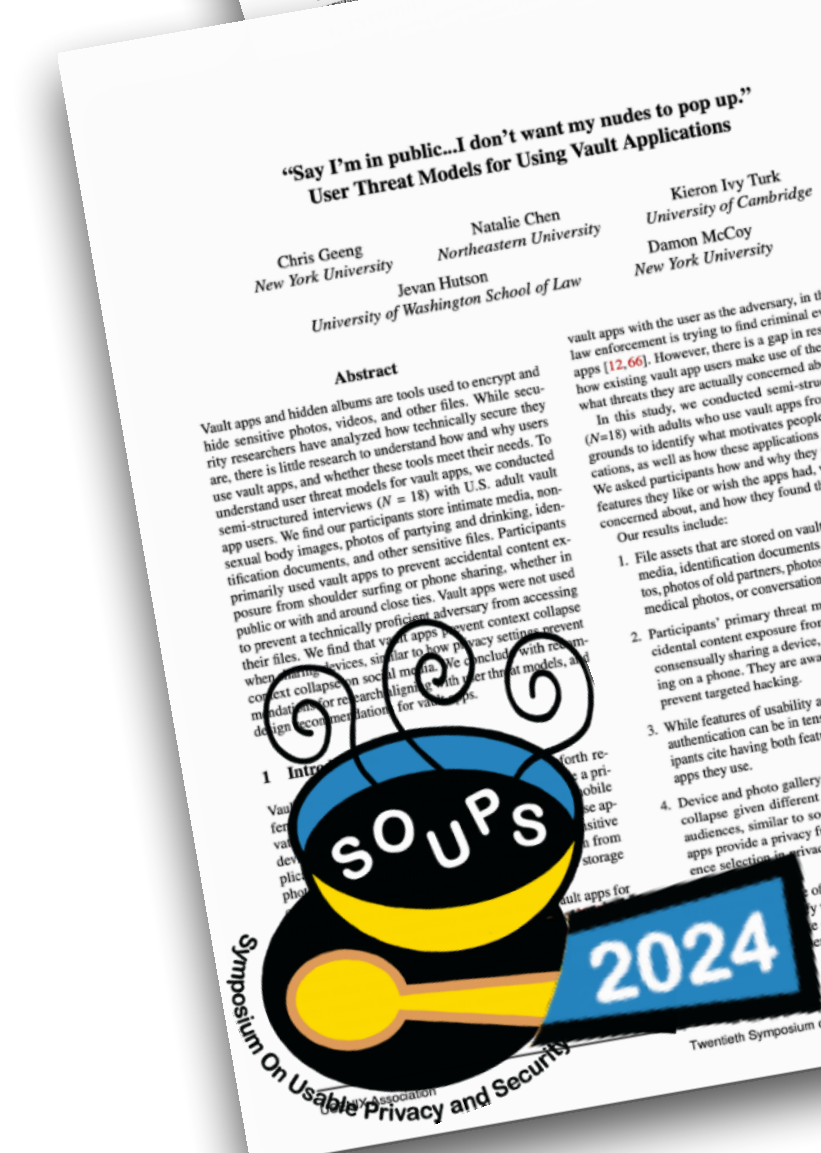
- Hassle free passwords

VPNs & proxy tools

- People believe in VPN privacy protections

antivirus

- Reflects what ads say



S&P apps, quite positive!



personal diary & journal

app lock

password managers

VPNs & proxy tools

antivirus

• People like journaling

• Hide applications from

• Hassle free passwords

• People believe in VPN

• privacy protections

• Re

• Antiviruses have all of the above!

**"Privacy is not for me, it's for those rich women":
Performative Privacy Practices on Mobile Phones by
Women in South Asia**
Nitya Sambasivan, Karen Checkley, Anna Baloof, Neve Ahmed*, David Nemer*, Laura Sainy Gaytan-Lugo*,
Tara Matthews*, Sunny Corralvo, and Elizabeth Churchill
Google Inc., Mountain View, CA, USA
(nityasamba, karen, sccorralvo@google.com, echurchil@google.com)
Information Technology University, Pakistan
*North South University, Bangladesh
*North South University, Bangladesh
*University of Kentucky, USA
*University of Colorado, Mexico
*Universidad de Colima, Mexico
*Independent Researcher
sainy@uconn.edu
taramatthews@gmail.com

ABSTRACT
Women in South Asia own fewer personal devices like laptops and smartphones than men do in the world. Further, cultural expectations dictate that they should share mobile devices with family members. In this paper, we report on a qualitative study conducted in India, Pakistan, and Bangladesh to understand how women use their personal mobile devices and how they manage privacy on these devices. We describe a set of five privacy practices and how they are implemented. These practices include: (1) using a separate user profile on the device, (2) using a separate app for social media, (3) using a separate browser for social media, (4) using a separate browser for social media, and (5) using a separate browser for social media. We discuss the implications of these practices for privacy and security on mobile devices.

**"Say I'm in public...I don't want my nudes to pop up."
User Threat Models for Using Vault Applications**
Chris Geeng, Natalis Chen, Kieron Ivy Turk
New York University, Northeastern University, University of Cambridge
Jevan Hutson, Damon McCoy
University of Washington School of Law, New York University

Abstract
Vault apps and hidden albums are tools used to encrypt and hide sensitive photos, videos, and other files. While security researchers have analyzed how technically secure these apps are, there is little research on understanding how and why users use vault apps, and whether these tools meet their needs. To understand user threat models for vault apps, we conducted semi-structured interviews (N = 18) with U.S. adult vault app users. We find our participants were primarily concerned with preventing accidental content exposure from shoulder surfing or phone sharing, whether in public or with and around close ties. Vault apps were not used primarily to prevent a technically proficient adversary from accessing their files. We find that participants were primarily concerned with preventing a technically proficient adversary from accessing their files. We find that participants were primarily concerned with preventing a technically proficient adversary from accessing their files.

Investigating Influencer VPN Ads on YouTube
Omer Akgul, Richard Roberts, Moses Namara*, Dave Levin, Michelle L. Mazurek
University of Maryland, *Clemson University

Abstract—One widespread, but frequently overlooked, source of security information is influencer marketing ads on YouTube. This paper examines how privacy products such as VPNs, proxy tools, and password managers are advertised on YouTube. Using a random sample of 1.4% of YouTube videos, we identify 243 unique VPN ads with a total of 63 million views. Our study concerns a subset of these ads, specifically those that promote security products. We analyze these ads to understand how they are advertised and how they are perceived by users. We find that these ads are often targeted to specific audiences and are often used to promote security products. We discuss the implications of these ads for privacy and security on YouTube.



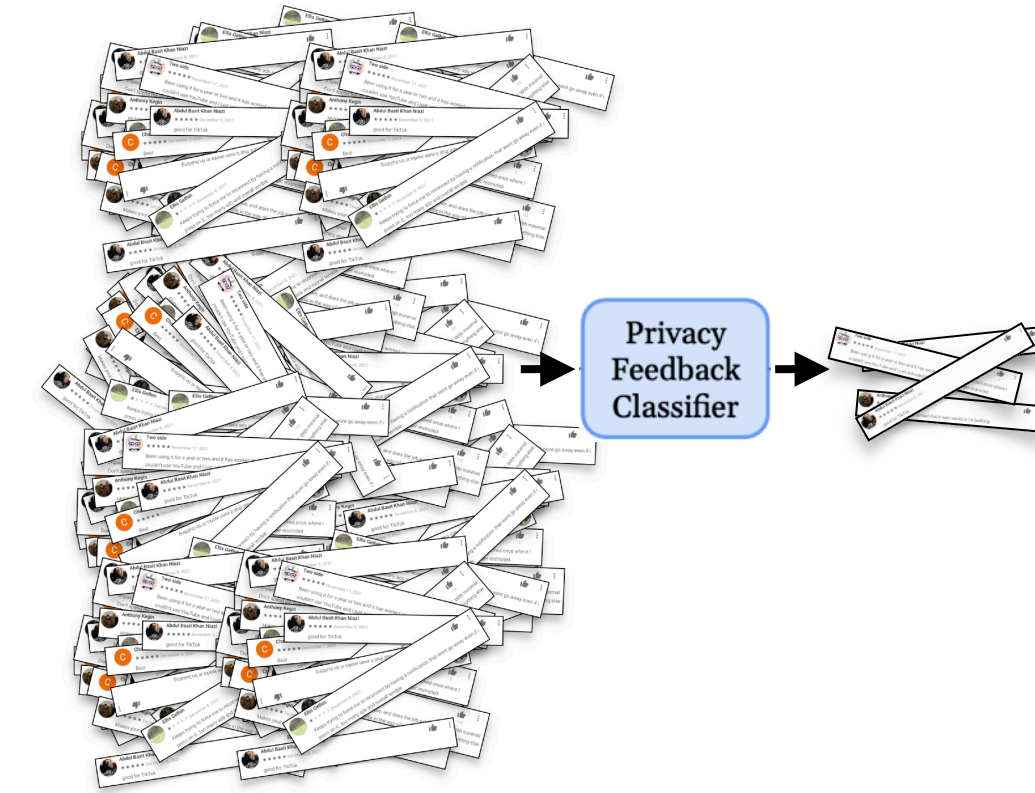
A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

- Our methods enable large scale analysis, uncovering issues broad and deep

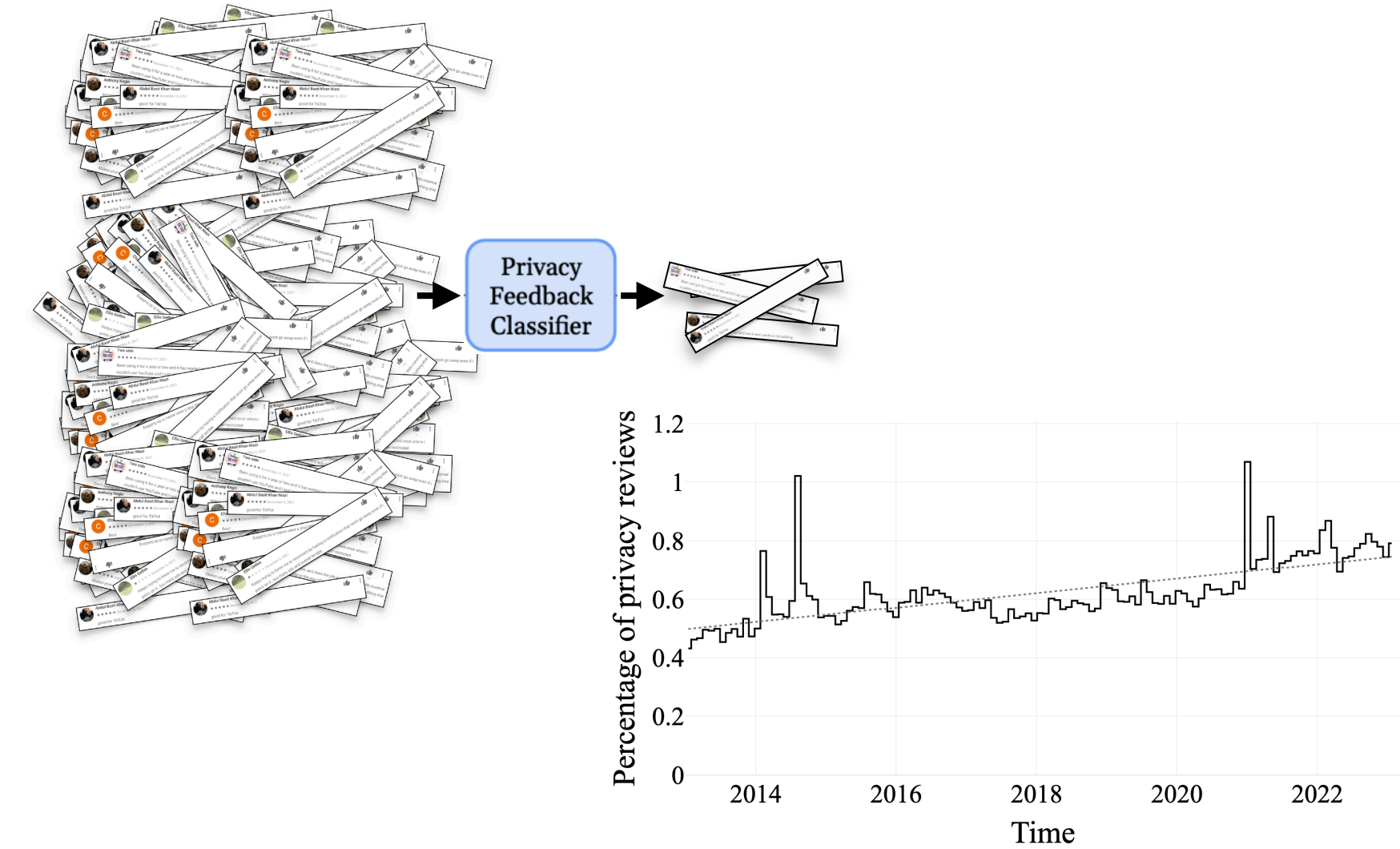
A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

- Our methods enable large scale analysis, uncovering issues broad and deep
- ~2B public Play reviews -> 12.3M privacy reviews



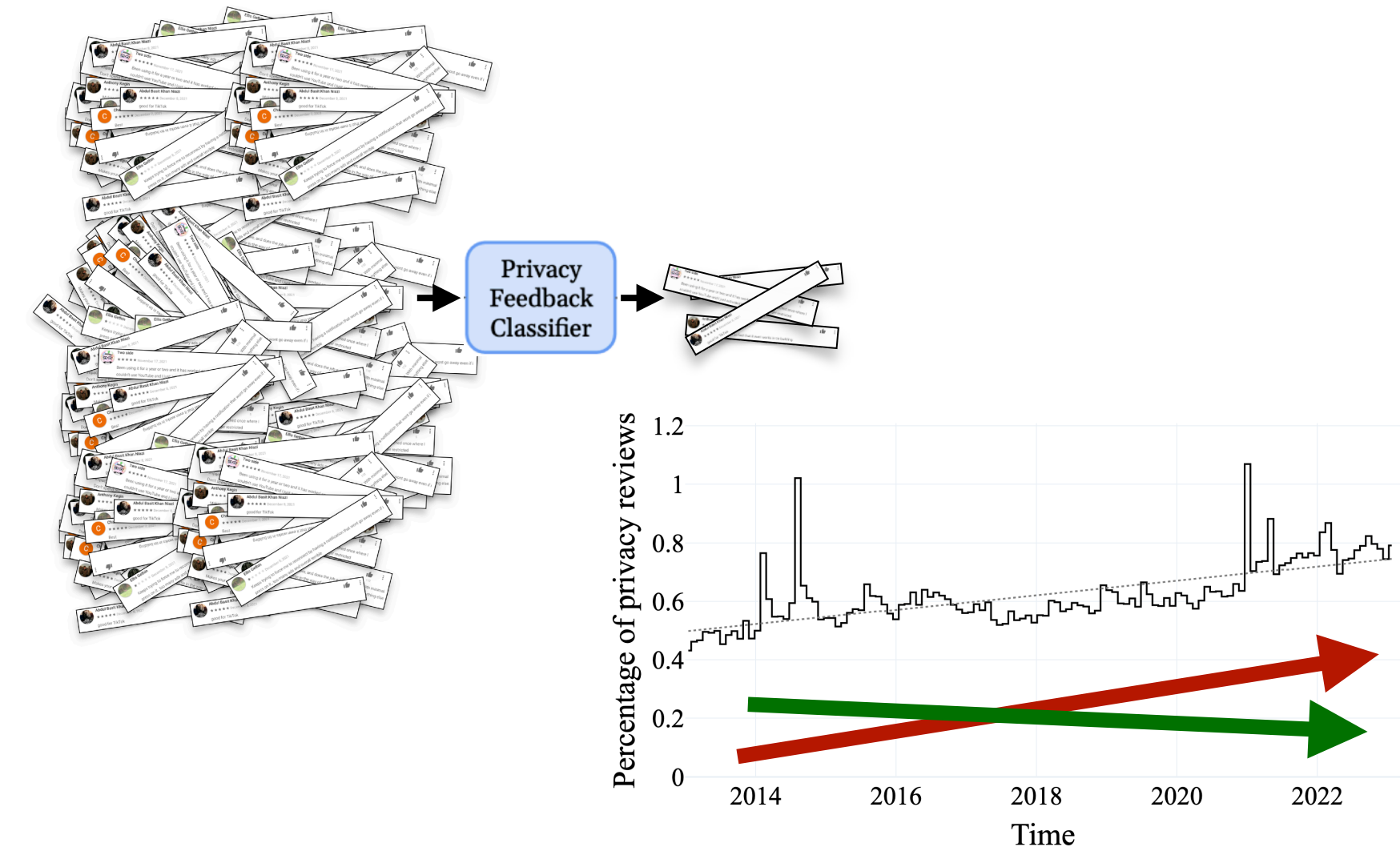
A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

- Our methods enable large scale analysis, uncovering issues broad and deep
- ~2B public Play reviews -> 12.3M privacy reviews
- Privacy reviews are up, but varies across dimensions



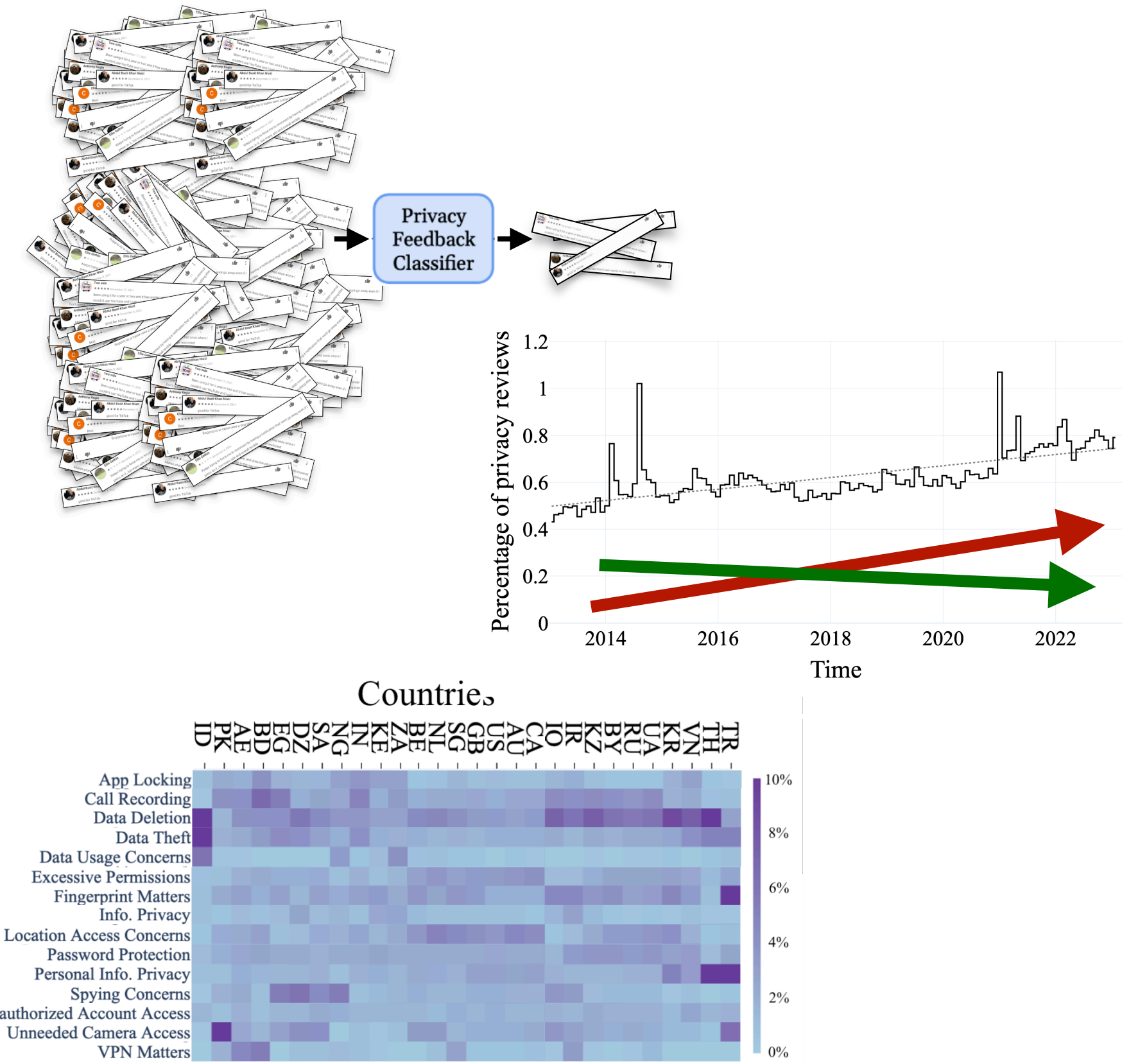
A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

- Our methods enable large scale analysis, uncovering issues broad and deep
- ~2B public Play reviews -> 12.3M privacy reviews
- Privacy reviews are up, but varies across dimensions



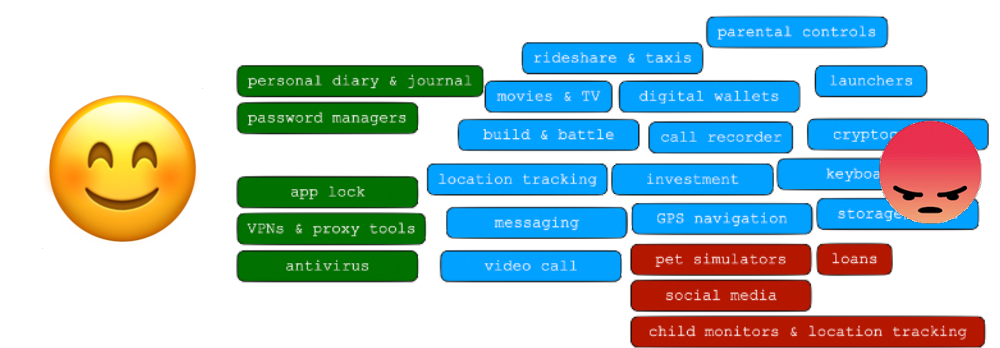
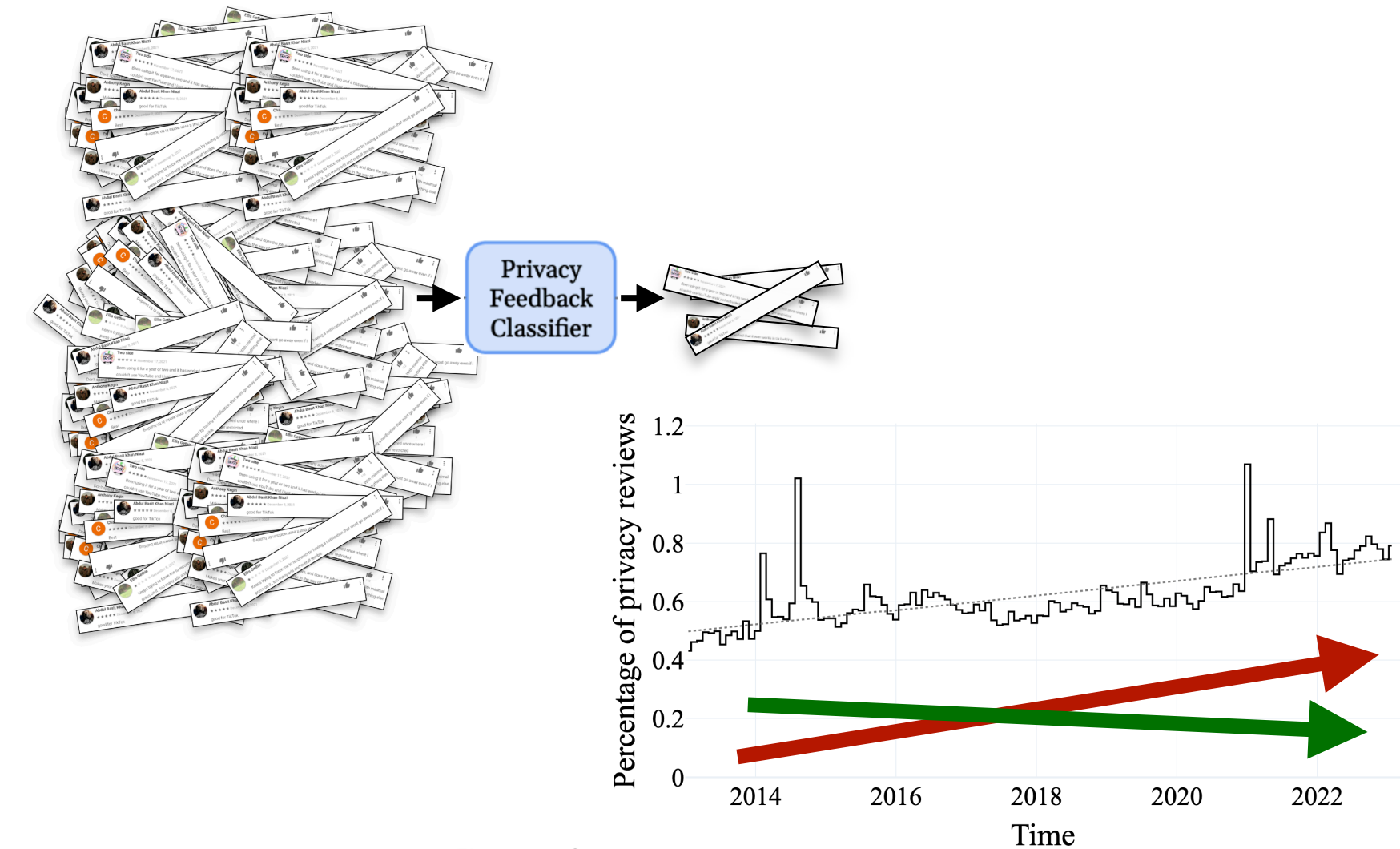
A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

- Our methods enable large scale analysis, uncovering issues broad and deep
- ~2B public Play reviews -> 12.3M privacy reviews
- Privacy reviews are up, but varies across dimensions
- Countries loosely group, but many unique issues



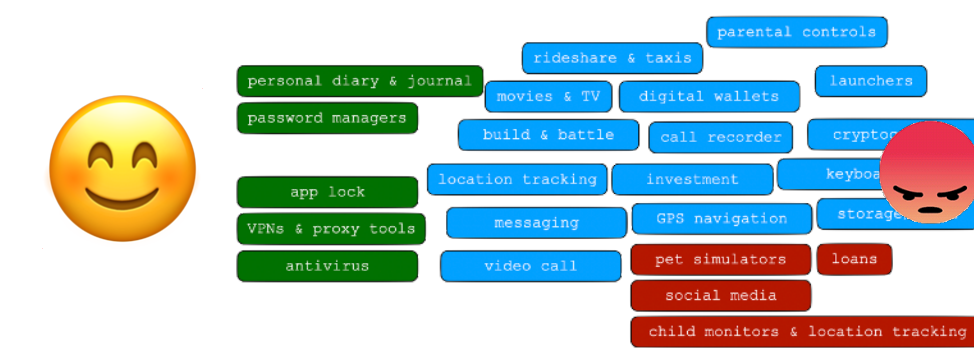
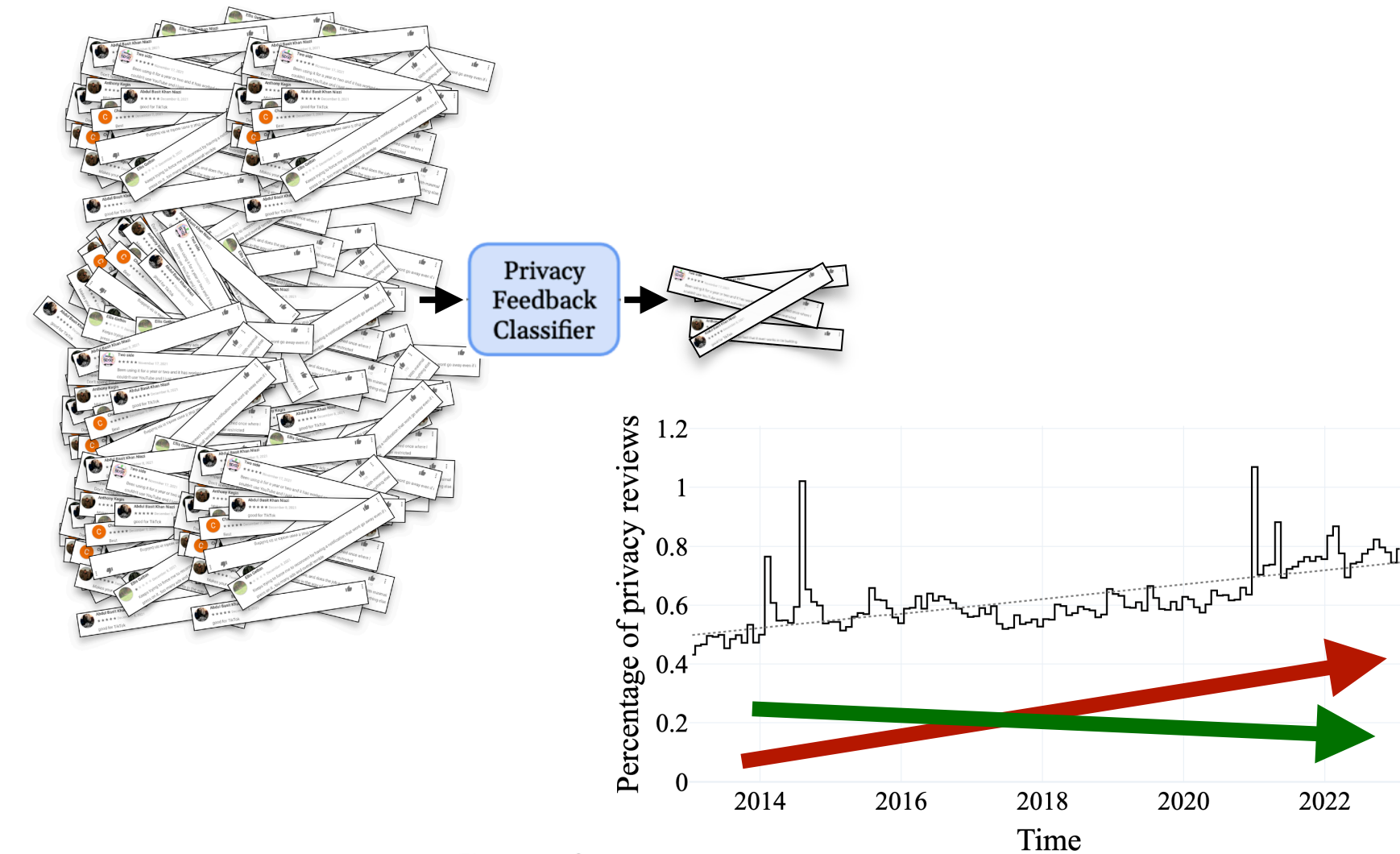
A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

- Our methods enable large scale analysis, uncovering issues broad and deep
- ~2B public Play reviews -> 12.3M privacy reviews
- Privacy reviews are up, but varies across dimensions
- Countries loosely group, but many unique issues
- S&P applications get really positive feedback



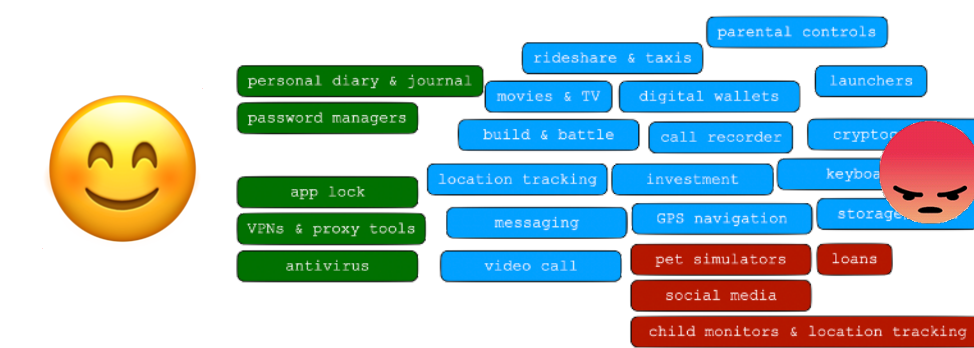
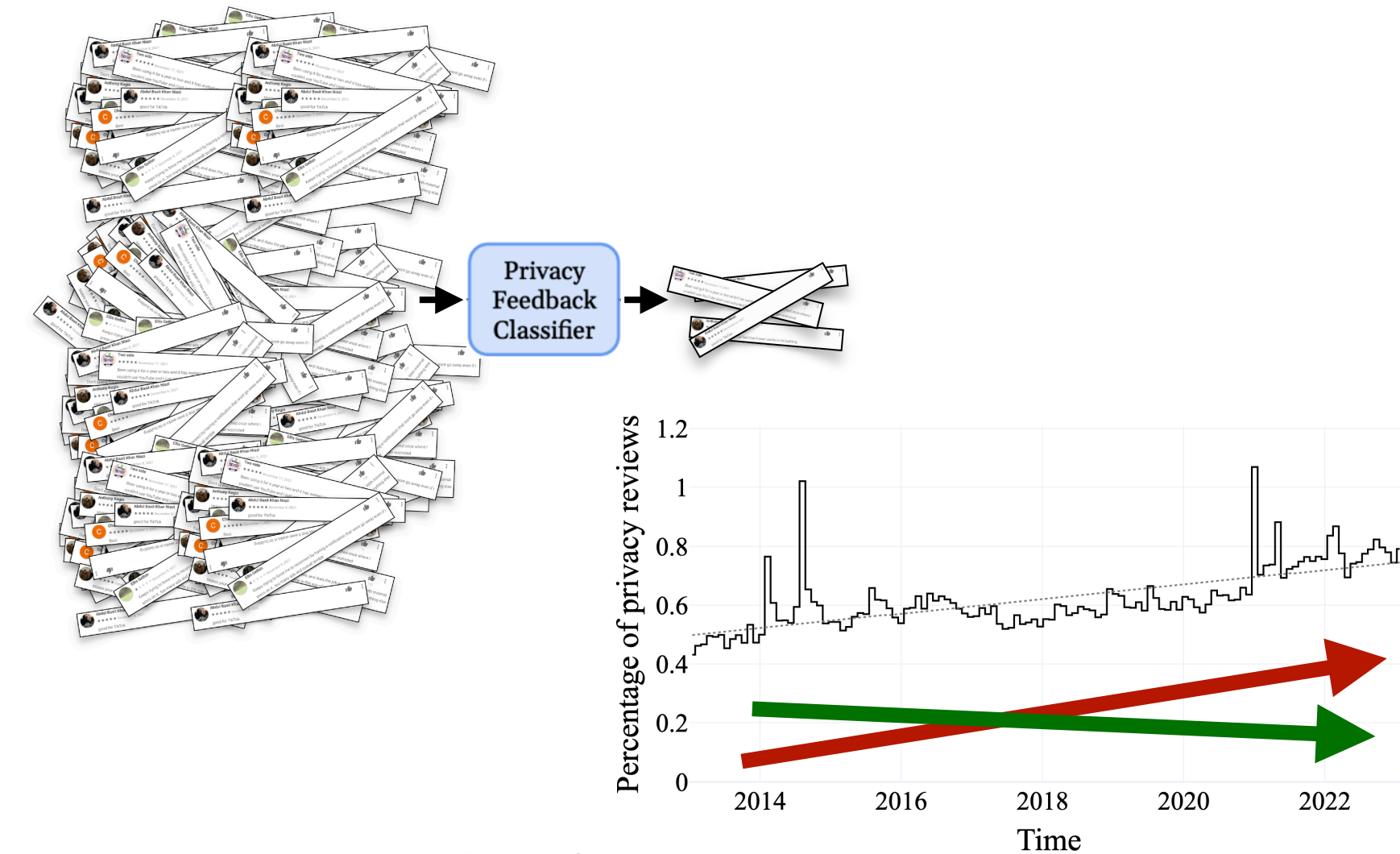
A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

- Our methods enable large scale analysis, uncovering issues broad and deep
- ~2B public Play reviews -> 12.3M privacy reviews
- Privacy reviews are up, but varies across dimensions
- Countries loosely group, but many unique issues
- S&P applications get really positive feedback
- We add context to prior work, uncover new issues, and highlight under researched areas

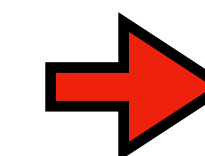


A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends

- Our methods enable large scale analysis, uncovering issues broad and deep
- ~2B public Play reviews -> 12.3M privacy reviews
- Privacy reviews are up, but varies across dimensions
- Countries loosely group, but many unique issues
- S&P applications get really positive feedback
- We add context to prior work, uncover new issues, and highlight under researched areas



Questions?



✉ oakgul@cmu.edu
 @_oakgul