GDPR COMPLIANCE FOR YOUR DATASTORE

PHILIPP KRENN

@XERAA

GDPR COMPLIANCE FOR YOUR DATASTORE

[redacted] [redacted]

elastic [redacted]

I DON'T KNOW HOW TO PUT THIS BUT...
GDPR IS KIND OF A BIG DEAL

WHO LIKES GDPR?

WHO IS AFRAID OF GDPR?

"CAN YOU RECOMMEND A GDPR EXPERT?

YES!

GREAT, CAN YOU GIVE ME THEIR EMAIL ADDRESS SO I CAN CONTACT THEM?

NO."

https://twitter.com/wardrox/status/988363811479572483

QUESTIONS:
HTTPS://SLI.DO/XERAA

ANSWERS:
HTTPS://TWITTER.COM/XERAA

GENERAL DATA PROTECTION REGULATION

ADOPTED 2016/04/14
ENFORCEABLE 2018/05/25

DATENSCHUTZ-GRUNDVERORDNUNG

FINES UP TO 4% OF GLOBAL REVENUES OR €20M

WHERE & WHO?

EU ORGANIZATIONS

SERVICES OR GOODS FOR / MONITORING OF EU CITIZENS

WHAT?

PERSONAL DATA

ANY INFORMATION RELATING TO AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON

RIGHTS?

TO BE INFORMED

ACCESS

RECTIFICATION

RIGHTS?

ERASURE (TO BE FORGOTTEN)

RESTRICT PROCESSING

DATA PORTABILITY

RIGHTS?

OBJECT

AUTOMATIC DECISION MAKING

PS: PERSONAL DATA IN A BLOCKCHAIN IS AN ISSUE

LAWFUL USE OF DATA?

INFORMED CONSENT

CONTRACTUAL OBLIGATION

LEGITIMATE INTEREST

LAWFUL USE OF DATA?

LEGAL OBLIGATION

VITAL INTERESTS

PUBLIC TASK

PROOF REQUIRED

RIGHT TO COLLECT AND LEGALLY USE

DISCLOSURE

WITHIN 72 HOURS TO A MEMBER STATE'S "SUPERVISORY BODY"

LEGACY DATA

STOP,
CHECK,
DELETE

LOOK RIGHT HERE
PREPARING FOR GDPR
imgflip.com

WHAT IF NO LEGAL GROUNDS?

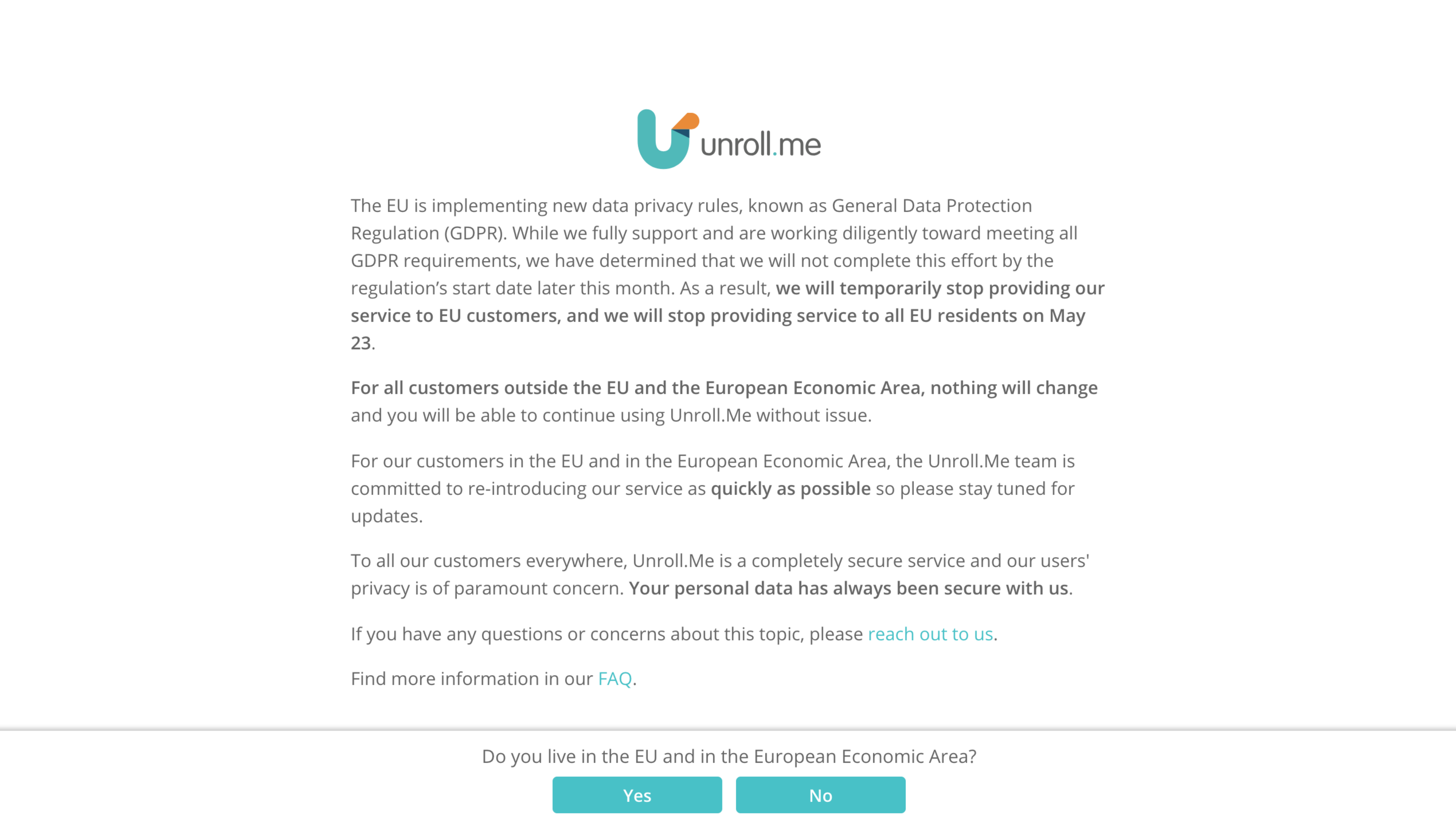
“MORE GDPR BIZARRO WORLD LOGIC. LOG NOTHING, BUT ALSO MAKE SURE TO HAVE A COMPLETE UNDERSTANDING OF ALL YOUR SECURITY BREACHES, TRACK THEM DOWN, PATCH THEM UP.... WITH NO LOGS.”

https://twitter.com/ianlandsman/status/997561351009599488

1. STOP YOUR SERVICE

Los Angeles Times

Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.



The EU is implementing new data privacy rules, known as General Data Protection Regulation (GDPR). While we fully support and are working diligently toward meeting all GDPR requirements, we have determined that we will not complete this effort by the regulation's start date later this month. As a result, **we will temporarily stop providing our service to EU customers, and we will stop providing service to all EU residents on May 23**.

For all customers outside the EU and the European Economic Area, nothing will change and you will be able to continue using Unroll.Me without issue.

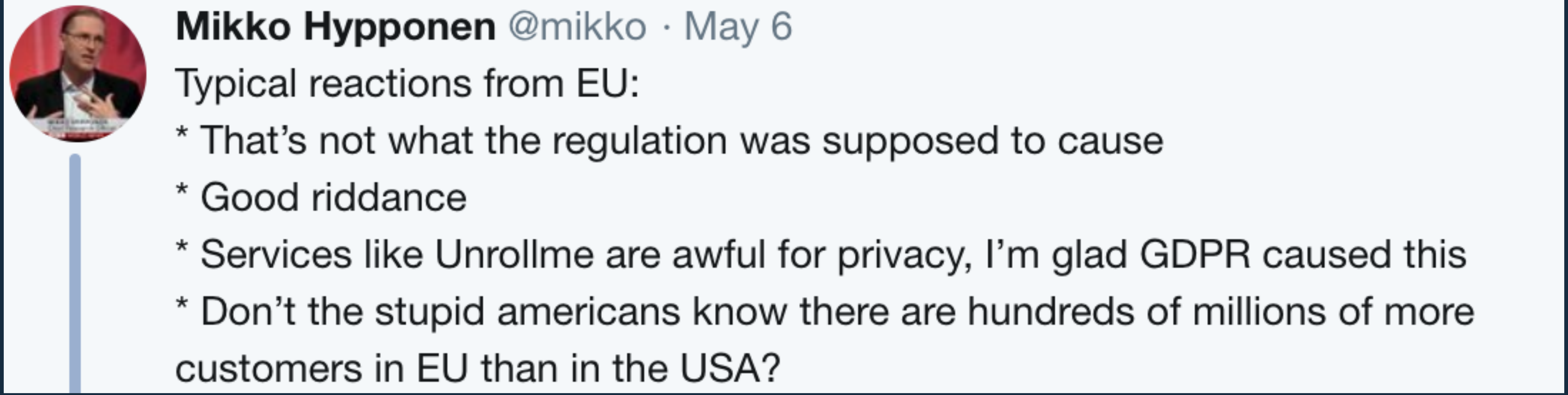
For our customers in the EU and in the European Economic Area, the Unroll.Me team is committed to re-introducing our service as **quickly as possible** so please stay tuned for updates.

To all our customers everywhere, Unroll.Me is a completely secure service and our users' privacy is of paramount concern. **Your personal data has always been secure with us**.

If you have any questions or concerns about this topic, please reach out to us.

Find more information in our FAQ.

Do you live in the EU and in the European Economic Area?



Mikko Hypponen @mikko · May 6

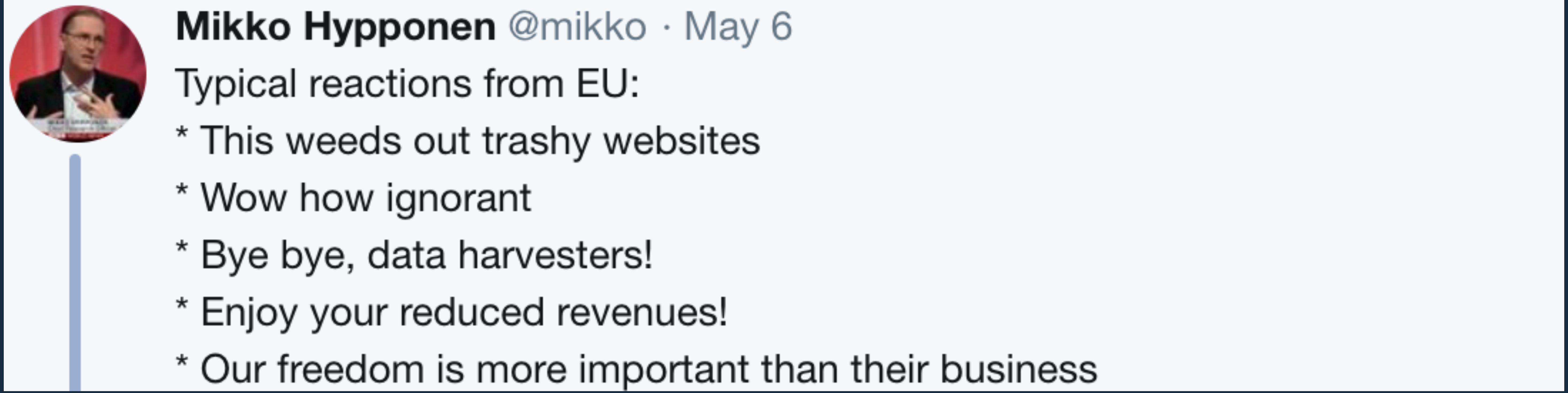
Typical reactions from EU:

* That’s not what the regulation was supposed to cause

* Good riddance

* Services like Unrollme are awful for privacy, I’m glad GDPR caused this

* Don’t the stupid americans know there are hundreds of millions of more customers in EU than in the USA?



Mikko Hypponen @mikko · May 6

Typical reactions from EU:

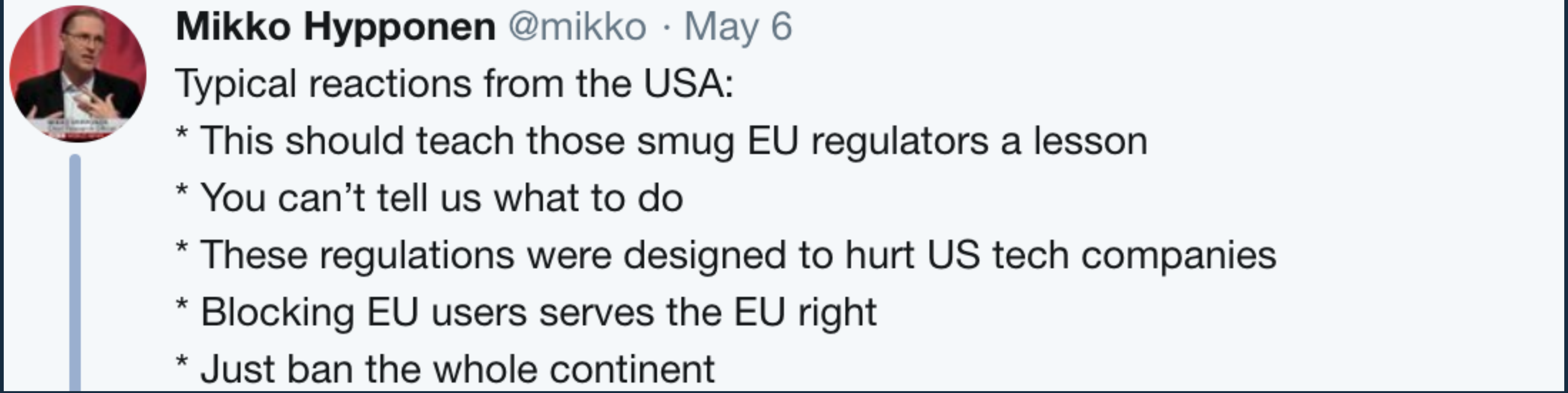
* This weeds out trashy websites

* Wow how ignorant

* Bye bye, data harvesters!

* Enjoy your reduced revenues!

* Our freedom is more important than their business



Mikko Hypponen @mikko · May 6

Typical reactions from the USA:

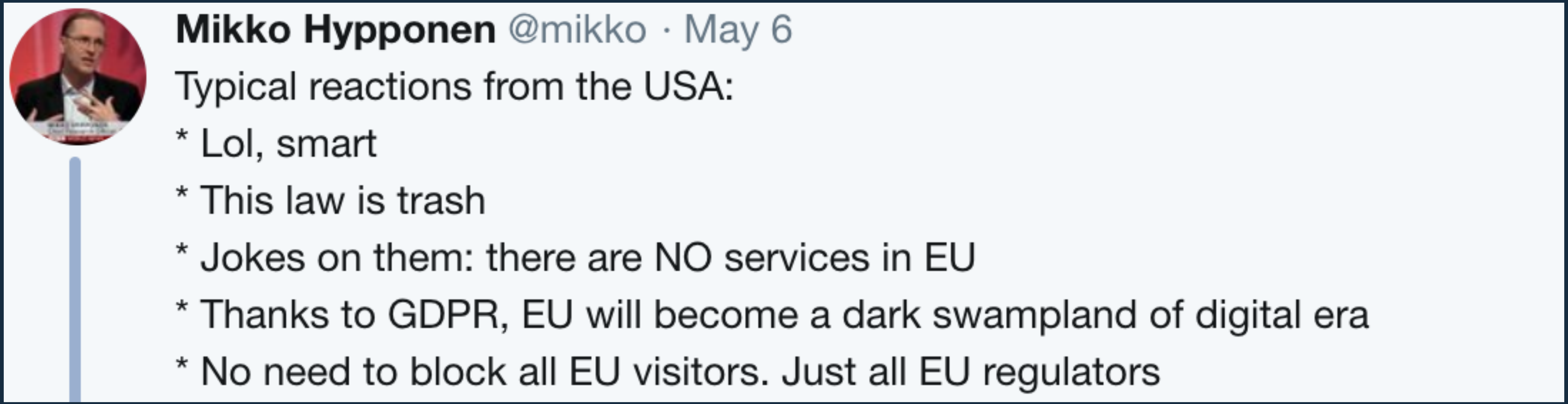
* This should teach those smug EU regulators a lesson

* You can’t tell us what to do

* These regulations were designed to hurt US tech companies

* Blocking EU users serves the EU right

* Just ban the whole continent



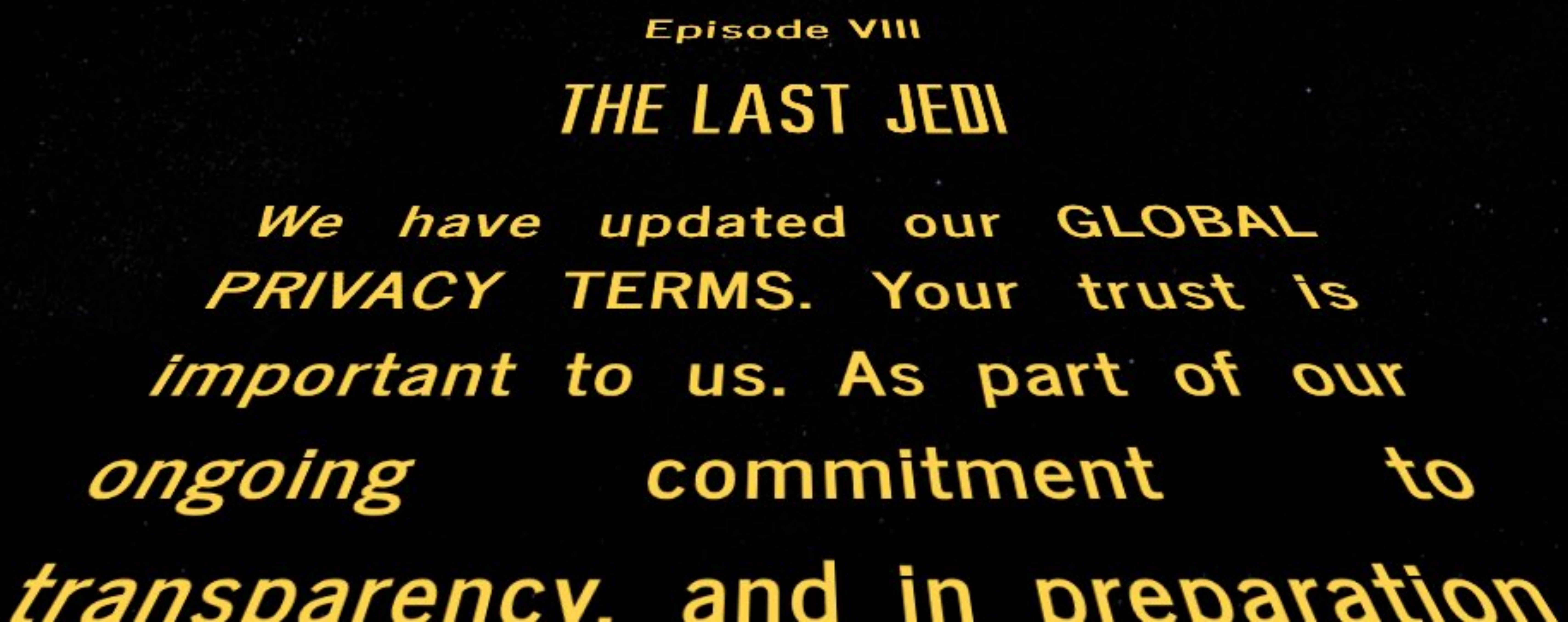
Mikko Hypponen @mikko · May 6

Typical reactions from the USA:

* Lol, smart
* This law is trash
* Jokes on them: there are NO services in EU
* Thanks to GDPR, EU will become a dark swampland of digital era
* No need to block all EU visitors. Just all EU regulators

2. DROWN THEM IN FORMS

HTTPS://TWITTER.COM/RIANJOHNSON/STATUS/999730569641525248



Episode VIII

THE LAST JEDI

We have updated our GLOBAL PRIVACY TERMS. Your trust is important to us. As part of our ongoing commitment to transparency, and in preparation

3. PSEUDONYMIZATION

ANONYMOUS

NO INFORMATION THAT COULD POTENTIALLY IDENTIFY AN INDIVIDUAL

NOT CONSIDERED PERSONAL DATA BY GDPR

PSEUDONYMOUS

RE-IDENTIFICATION POSSIBLE IF COMBINED WITH ADDITIONAL INFORMATION

WITHOUT THIS INFORMATION, RE-IDENTIFICATION PRACTICALLY IMPOSSIBLE

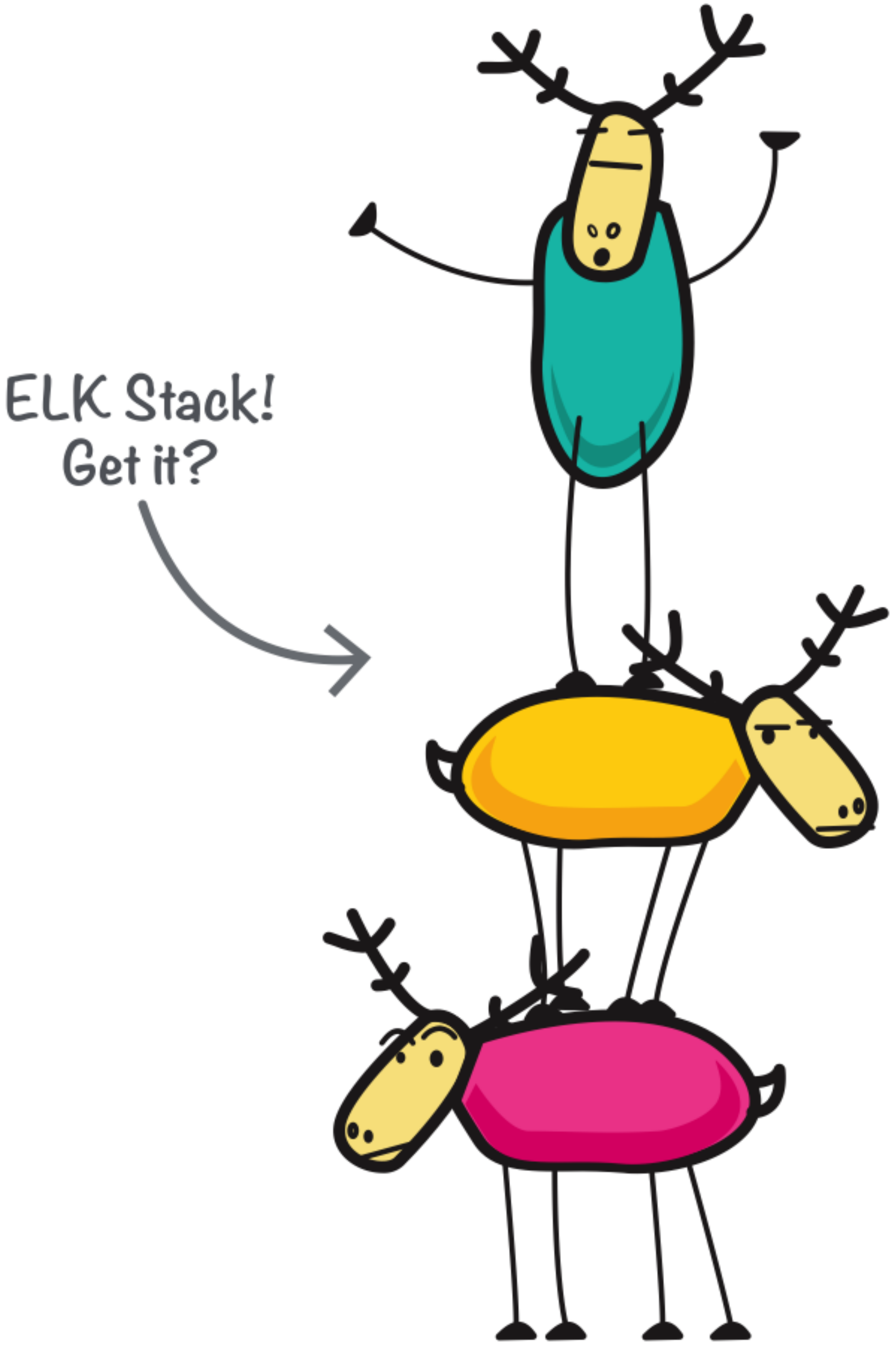
WHEN?

INGESTION TIME

SEARCH TIME

elastic

DEVELOPER 🥑

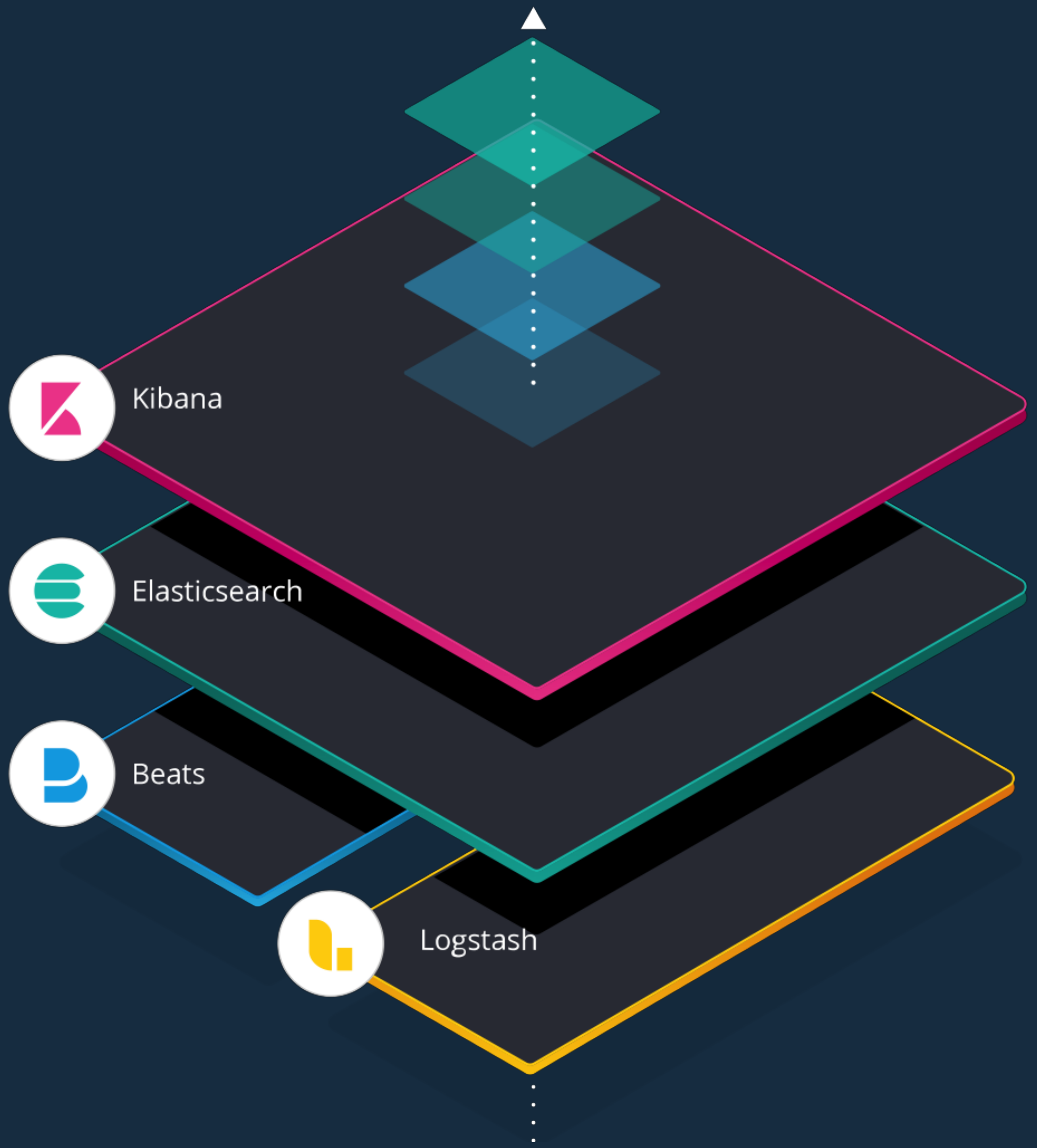


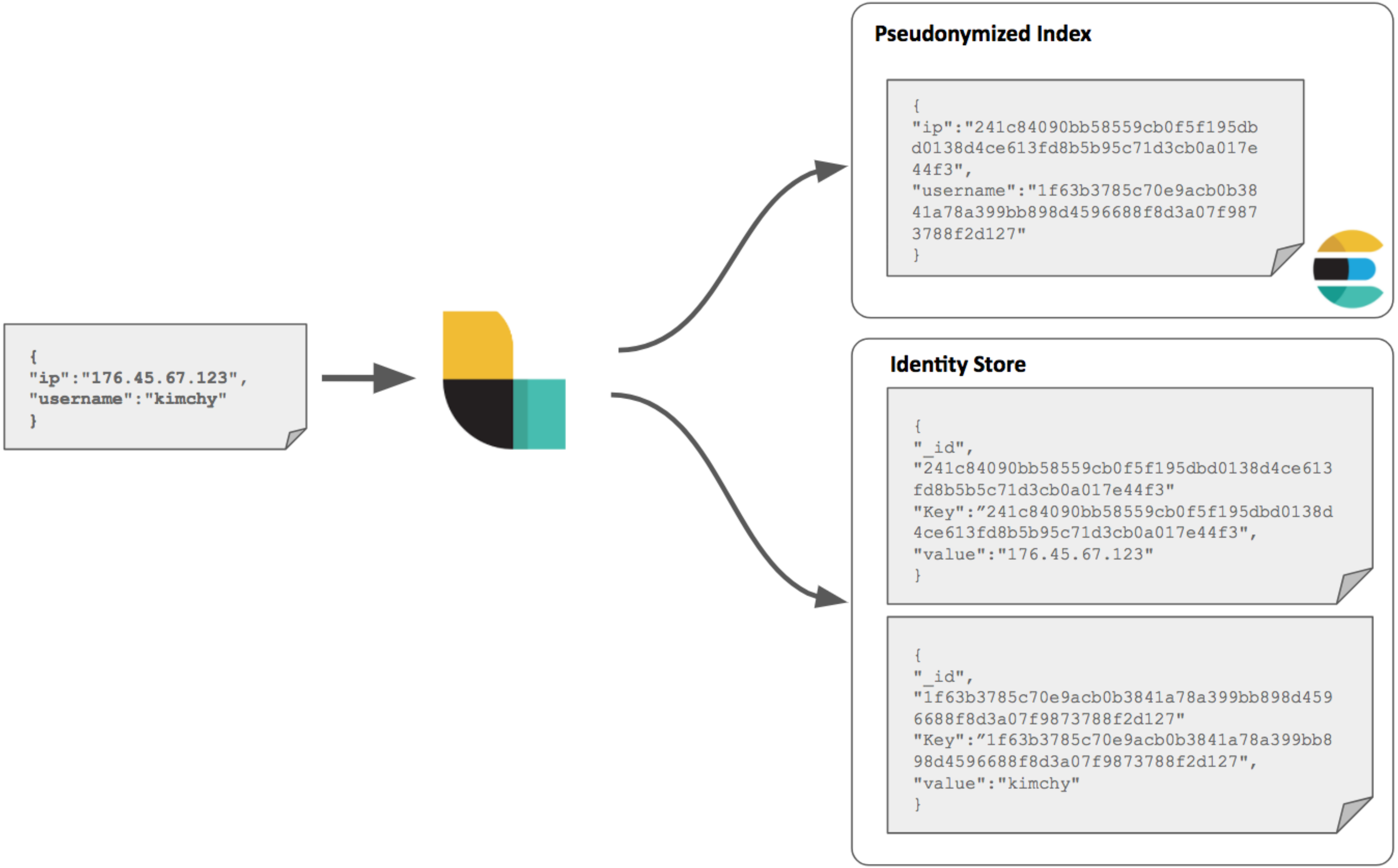
E Elasticsearch

L Logstash

K Kibana

elastic stack


Kibana
Elasticsearch
Beats
Logstash



```
{
"ip":"176.45.67.123",
"username":"kimchy"
}
```

Pseudonymized Index

```
{
"ip":"241c84090bb58559cb0f5f195db
d0138d4ce613fd8b5b95c71d3cb0a017e
44f3",
"username":"1f63b3785c70e9acb0b38
41a78a399bb898d4596688f8d3a07f987
3788f2d127"
}
```

Identity Store

```
{
"_id",
"241c84090bb58559cb0f5f195dbd0138d4ce613
fd8b5b5c71d3cb0a017e44f3"
"Key":”241c84090bb58559cb0f5f195dbd0138d
4ce613fd8b5b95c71d3cb0a017e44f3",
"value":"176.45.67.123"
}
```

```
{
"_id",
"1f63b3785c70e9acb0b3841a78a399bb898d459
6688f8d3a07f9873788f2d127"
"Key":”1f63b3785c70e9acb0b3841a78a399bb8
98d4596688f8d3a07f9873788f2d127",
"value":"kimchy"
}
```

```
fingerprint {
    method => "SHA256"
    source => ["ip"]
    key => "${FINGERPRINT_KEY}"
}

mutate {
      add_field => {
          '[identities][0][key]' => "%{fingerprint}"
          '[identities][0][value]' => "%{ip}"
      }
}

mutate {
    replace => {
        "ip" => "%{fingerprint}"
    }
}
```

HOW SECURE ARE HASHES?

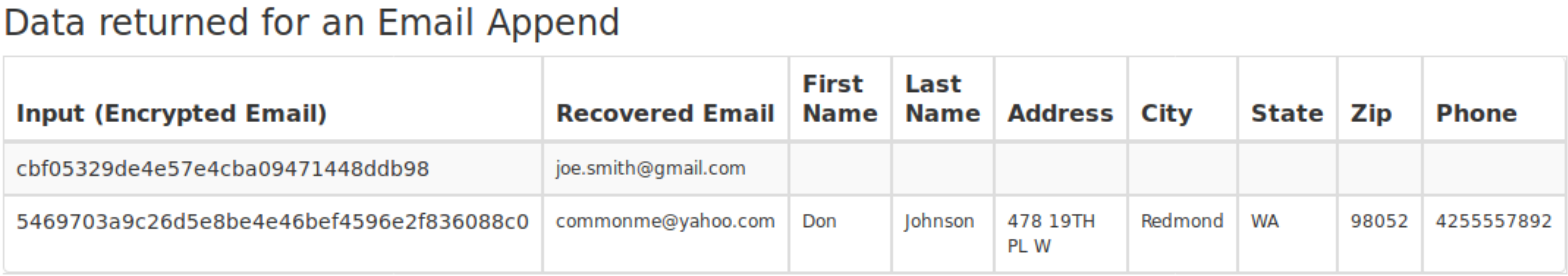
WITHOUT SALTING

> “YOU MIGHT THINK IT WOULD TAKE A LONG TIME TO RUN THROUGH ALL OF THE POSSIBLE SSNS, BUT COMPUTERS ARE VERY FAST — THERE ARE "ONLY" ONE BILLION POSSIBLE SSNS, SO YOUR LAPTOP CAN HASH ALL OF THEM IN LESS TIME THAN IT TAKES YOU TO GET A CUP OF COFFEE.”

https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous

“DATAFINDER – REVERSE EMAIL HASHES FOR $0.04 PER EMAIL”

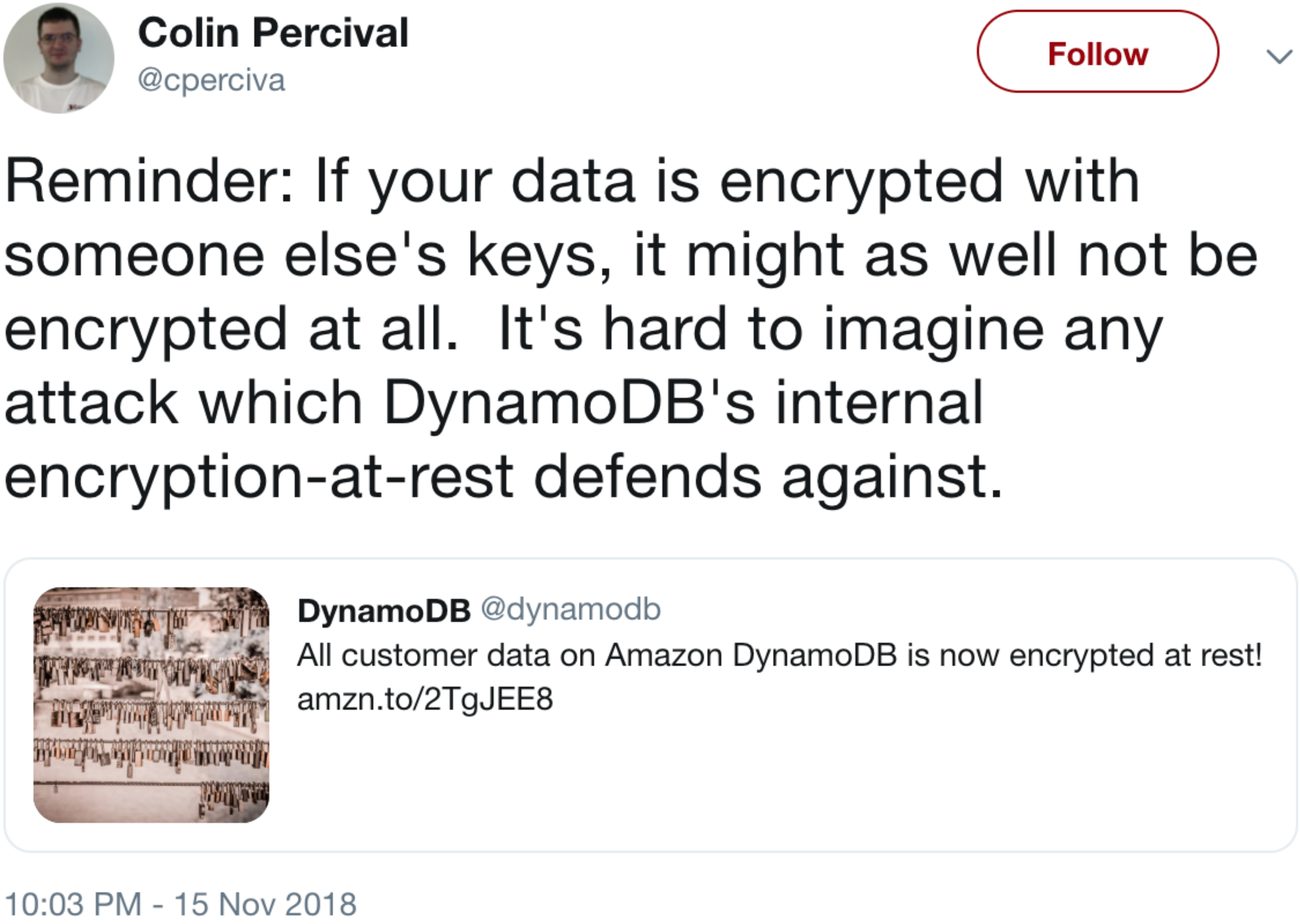
https://freedom-to-tinker.com/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/



Data returned for an Email Append

Input (Encrypted Email)	Recovered Email	First Name	Last Name	Address	City	State	Zip	Phone
cbf05329de4e57e4cba09471448ddb98	joe.smith@gmail.com							
5469703a9c26d5e8be4e46bef4596e2f836088c0	commonme@yahoo.com	Don	Johnson	478 19TH PL W	Redmond	WA	98052	4255557892

ACCESS CONTROL & ENCRYPTION



Colin Percival
@cperciva

Reminder: If your data is encrypted with someone else's keys, it might as well not be encrypted at all. It's hard to imagine any attack which DynamoDB's internal encryption-at-rest defends against.

DynamoDB @dynamodb
All customer data on Amazon DynamoDB is now encrypted at rest! amzn.to/2TgJEE8

10:03 PM - 15 Nov 2018

DELETION

“INTERESTING #GDPR SOLUTION FOR THE "RIGHT TO ERASURE" : ENCRYPT ALL USER'S DATA AND WHEN YOU HAVE TO DELETE IT YOU JUST GET RID OF THE PRIVATE KEY.

WILL THIS BECOME THE NORM?”

https://twitter.com/Stephan007/status/985103374118014976

“[...] PERSONAL DATA OF OUR USERS CAN ONLY BE PERSISTED WHEN IT IS ENCRYPTED. EACH USER HAS THEIR OWN SET OF KEYS

[...] IT REDUCES THE IMPACT OF LEAKING A DATASET, SINCE THE DATASET BY ITSELF IS USELESS — ATTACKERS ALSO NEED THE DECRYPTION KEYS.

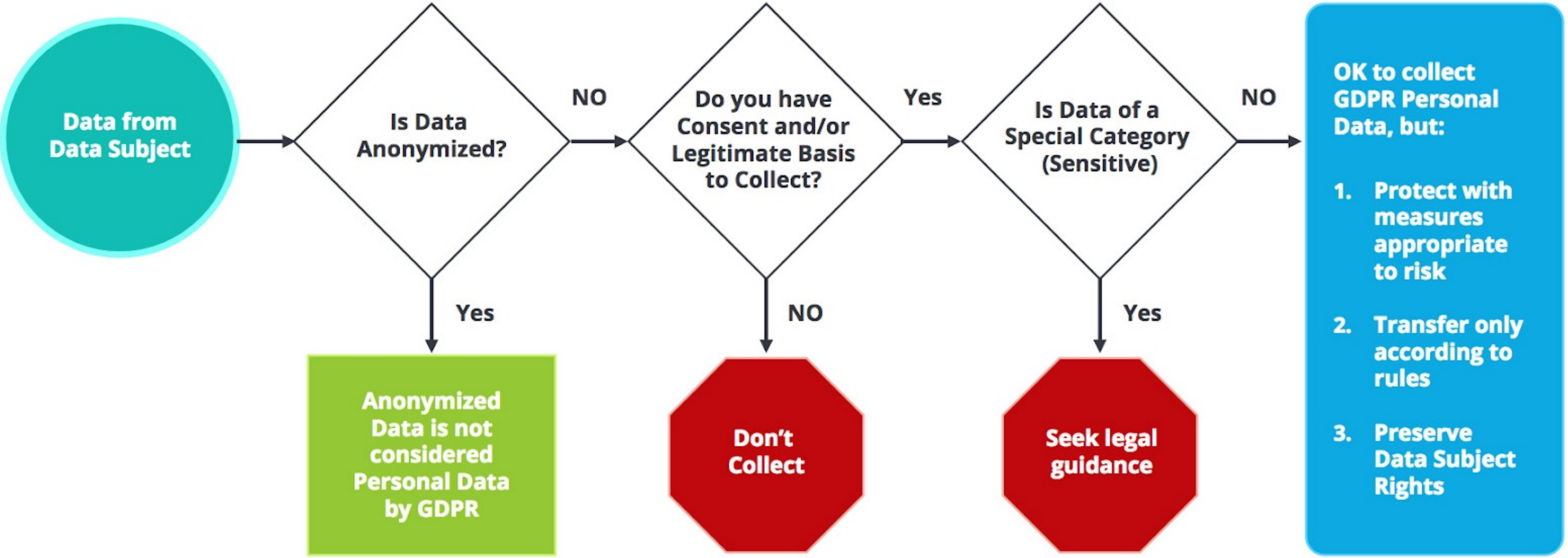
[...] IT ALLOWS US TO CONTROL THE LIFECYCLE OF DATA FOR INDIVIDUAL USERS CENTRALLY.”

https://labs.spotify.com/2018/09/18/scalable-user-privacy/

CONCLUSION

DATA PROTECTION

THE NEW STANDARD AND NORM OF APPROACHING PERSONAL DATA



Data from Data Subject

Is Data Anonymized?

Yes

Anonymized Data is not considered Personal Data by GDPR

NO

Do you have Consent and/or Legitimate Basis to Collect?

NO

Don't Collect

Yes

Is Data of a Special Category (Sensitive)

Yes

Seek legal guidance

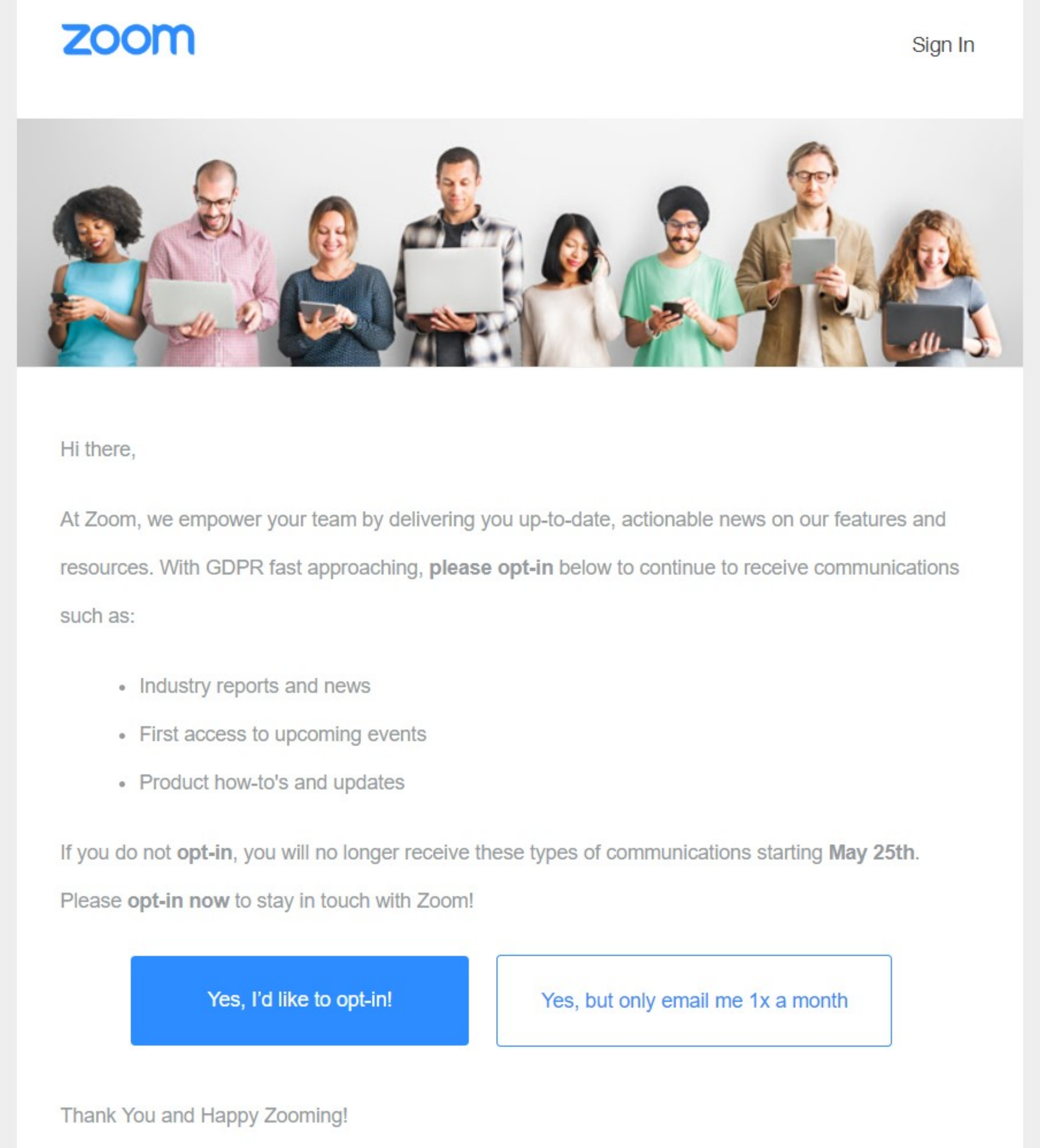
NO

OK to collect GDPR Personal Data, but:

1. Protect with measures appropriate to risk
2. Transfer only according to rules
3. Preserve Data Subject Rights

I AM NOT A LAWYER

❤️ GDPR AND CARRY ON



Hi there,

At Zoom, we empower your team by delivering you up-to-date, actionable news on our features and resources. With GDPR fast approaching, **please opt-in** below to continue to receive communications such as:

- Industry reports and news
- First access to upcoming events
- Product how-to's and updates

If you do not **opt-in**, you will no longer receive these types of communications starting **May 25th**.

Please **opt-in now** to stay in touch with Zoom!

Thank You and Happy Zooming!

QUESTIONS?

PHILIPP KRENN @XERAA