



joe

@mutablejoe

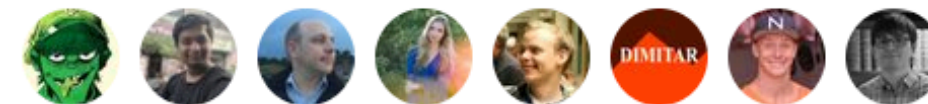
Follow



He's making a list
He's checking it twice
He's gonna find out who's naughty or nice
Santa Claus is in contravention of article 4 of
the General Data Protection Regulation (EU)
2016/679

9:39 AM - 20 May 2018

19,820 Retweets 45,057 Likes



The Seven GDPR Sins of Personal-Data Processing Systems

Supreeth Shastri, Melissa Wasserman, Vijay Chidambaram



General Data Protection Regulation (GDPR)

May 25, 2018

Adopted after 2 years of public debate.
All but 2 EU countries have legislated.

Fundamental right

Grants all European people a right to protection and privacy of personal data

Personal data

Any information relating to a natural person;
Broad in scope unlike FERPA, HIPAA

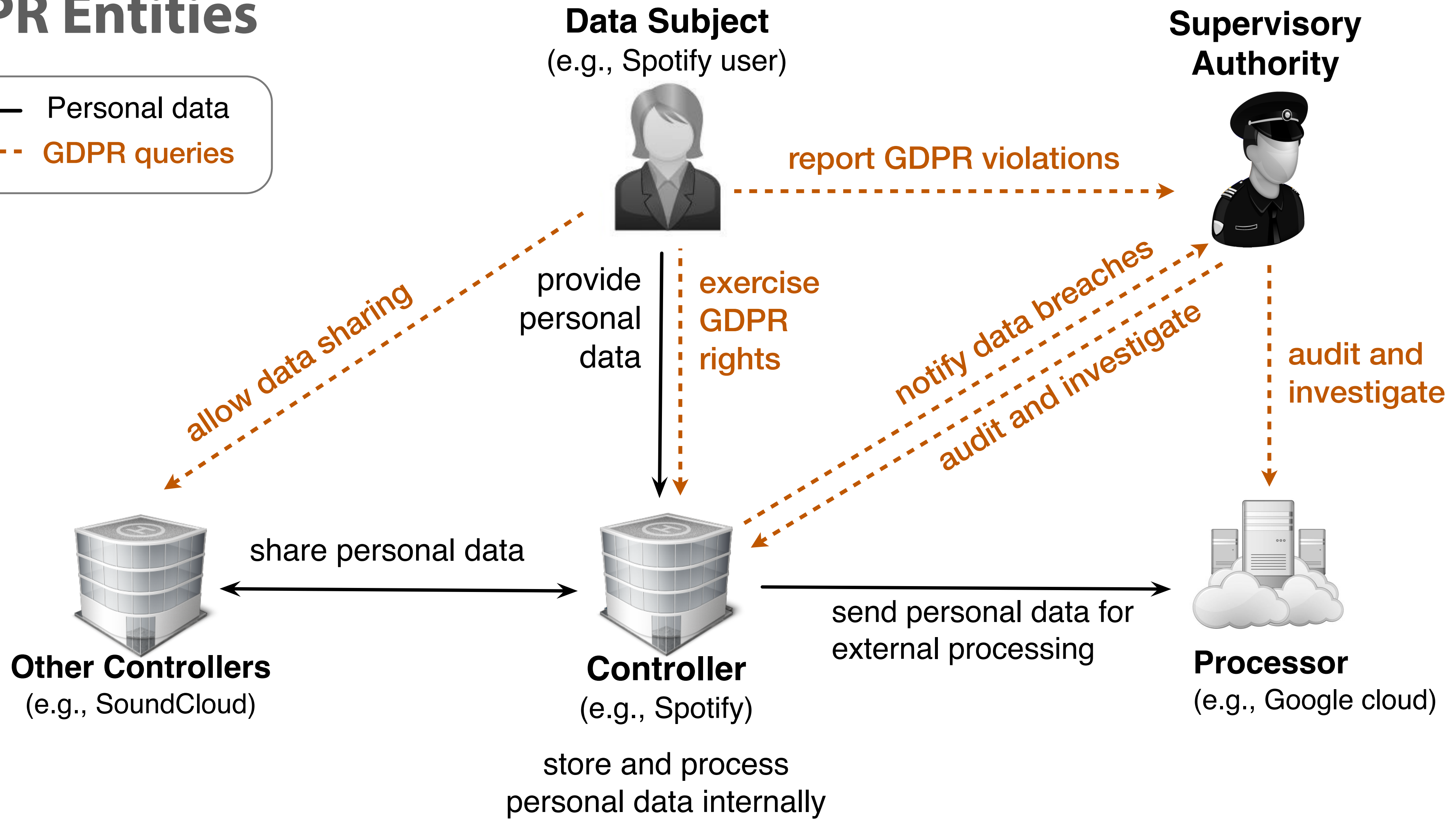
Covers entire lifecycle

Collection, processing, protection, transfer and deletion; Regulated via 99 articles

Hefty penalty

Max penalty of 4% of global revenue or €20 million, whichever is greater

GDPR Entities



GDPR in the Wild



Internet-era systems have **primarily** focused on reliability, scalability, and affordability.



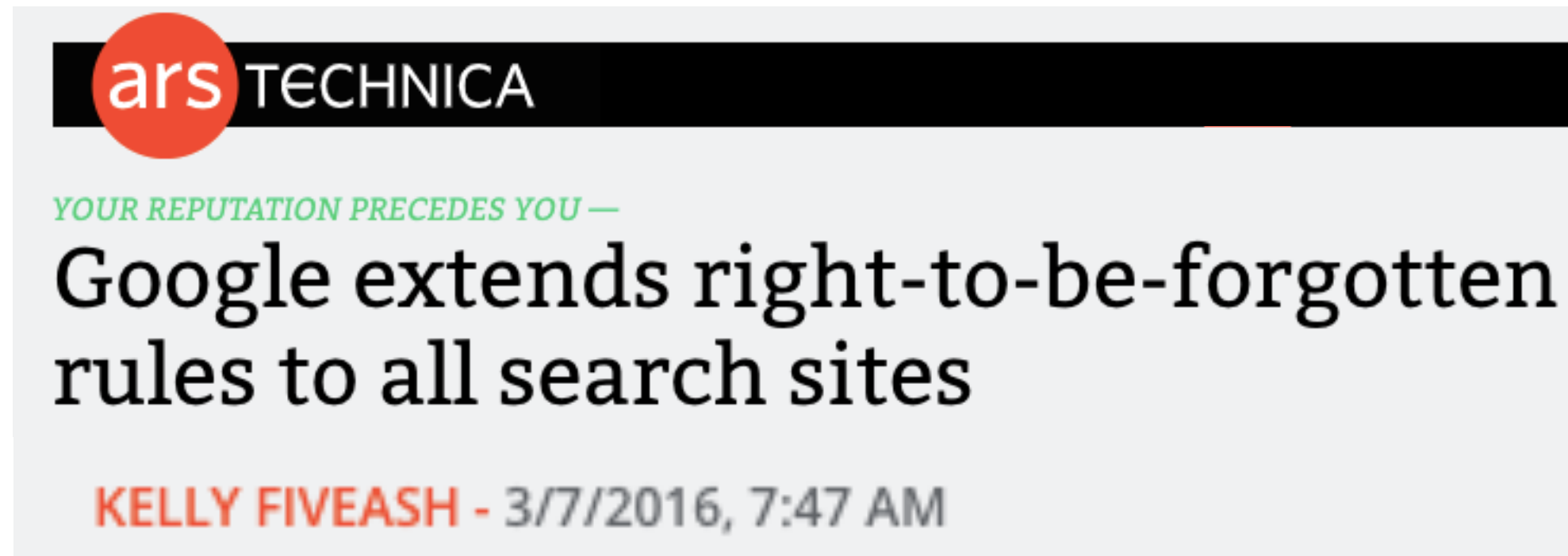
**KEY
OBSERVATION**

Relegating security and privacy as afterthoughts has given rise to **principles** and **practices** that are **at odds** with **GDPR**.

The Seven GDPR Sins

1. Storing Data Forever

BEFORE



ars TECHNICA

YOUR REPUTATION PRECEDES YOU —

Google extends right-to-be-forgotten rules to all search sites

KELLY FIVEASH - 3/7/2016, 7:47 AM

§17: RIGHT TO BE FORGOTTEN

(1) The data subject shall have the right to obtain from the controller the erasure of personal data without undue delay [...]

AFTER

180
days

Time that **Google cloud** requires to guarantee that a requested personal data item is fully deleted

§ 5(1)(E): STORAGE LIMITATION

[...] kept for no longer than is necessary for the purposes for which the personal data are processed [...]

2. Reusing Data Indiscriminately

BEFORE



Facebook is using your 2FA phone number to target ads at you

Reported by GIZMODO on 9/26/2018

§ 5(1)(B): PURPOSE LIMITATION

"Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes [...]"

AFTER



On Jan 21st 2019, the French DPA levied the **largest** GDPR fine yet on **Google** for **purpose bundling**

§ 21: RIGHT TO OBJECT

"(1)The data subject shall have the right to object at any time to processing of personal data concerning him or her [...]"

3. Creating Black Markets and Walled Gardens

BEFORE

700B

Total personal data items accrued

3000+

Unique data points per US consumer

§14: INFORMATION TO BE PROVIDED WHERE PERSONAL DATA HAVE NOT BEEN OBTAINED FROM THE DATA SUBJECT

*"(1) (c) the purposes of the processing [...]. (e) the recipients [...].
(2) (a) the period for which the personal data will be stored [...].
(f) from which source the personal data originate [...]."*

AFTER



Many programmatic ad exchanges shut down



§ 20: RIGHT TO DATA PORTABILITY

"(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller. (2) [...] the right to have the personal data transmitted directly from one controller to another."

4. Risk Agnostic Data Processing (a.k.a Move fast and break Things)

BEFORE



§ 35: DATA PROTECTION IMPACT ASSESSMENT

"Where processing, in particular using new technologies, is likely to result in a high risk to the rights of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing."

AFTER



User accounts hacked in 2018, after Facebook's **View-As** feature was exploited.

§ 36: PRIOR CONSULTATION

"The controller shall consult the supervisory authority prior to processing where [...] it would result in a high risk in absence of measures taken by the controller to mitigate the risk."

5. Hiding Data Breaches

§ 33: NOTIFICATION OF A PERSONAL DATA BREACH

(1) the controller shall without undue delay and not later than 72 hours after having become aware of it, notify the supervisory authority. [...]

(3) The notification shall at least describe the nature of the personal breach, [...] likely consequences, and [...] measures taken to mitigate its adverse effects. "

Breaches in the real world

945

Before GDPR
(worldwide)

41,502

After GDPR
(only Europe)

Reported data breaches **6 months**
before and after GDPR

6. Making Unexplainable Decisions

BEFORE

The Atlantic

A Popular Algorithm Is No Better at Predicting Crimes Than Random People

The COMPAS tool is widely used to assess a defendant's risk of committing more crimes, but a new study puts its usefulness into perspective.

§ 22: AUTOMATED INDIVIDUAL DECISION-MAKING

"(1) The data subject shall have the right not to be subject to a decision based solely on automated processing [...]"

AFTER

ICML

Workshop on Human Interpretability in ML

IJCAI

Workshop on Explainable AI

§ 15: RIGHT OF ACCESS

"(1) The data subject shall have the right to obtain from the controller [...] meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing."

7. Security as a Secondary Goal

§ 25: DATA PROTECTION BY DESIGN AND BY DEFAULT

"(1) [...] design to implement data protection principles in an effective manner [...]"

§ 24: RESPONSIBILITY OF THE DATA CONTROLLER

"the controller shall [...] be able to demonstrate that processing is performed in accordance with this Regulation."

Security in the real world



ML-driven reactive security

Concluding Remarks

FUTURE DIRECTIONS

GDPR-compliant **Redis**
Exploring system-level tradeoff
in achieving compliance

Cloud consolidation
Could compliance be better
tackled at cloud provider level?

Beyond GDPR
California's CCPA is going
into effect 1/1/2020

We want to hear from you!



<https://utsaslab.github.io/research/gdpr/>