

GDPR-compliant face recognition?

CC BY-SA, Thomas Amberg, FHNW
(Screenshots considered fair use)

Home

20% 21%

Kate Crawford
@katecrawford

Researching the
Co-founder @AIN
Principal Research
Distinguished Res



Kate Crawford ✓

@katecrawford

Following

So who's got the best headline for the facial recognition ban?

"SAN FRAN BANS MAN SCANS"

"FACE TRACE HAS NO PLACE"

@jovialjoy @alvarombedoya @timnitGebru

@hartzog @EvanSelinger @onekade

@Matt_Cagle @wewatchwatchers

@mer__edith

12:22 AM - 15 May 2019

70 Retweets 370 Likes



51

70

370



Dr. S.A. Applin @AnthroPunk · May 16

Replying to @katecrawford @jovialjoy and 8 others

SF NIXES PIXELS



Tweet

Close

Dashboard

Dashboard

AI Ethics @ PARC

Home

Committee Guidelines

AI Ethics Checklist

Mission Statement

Mechanics

Physical Interaction

Physical interaction should be thought of broadly including machinery and also any kind of sensors or actuators.

Question	Yes	No
Is there heavy equipment or is it operating at high speed?		
For cameras, microphones, sensors, or anything that records human likenesses or activity:		
Is it in a public place?		
Is it hidden from anyone who might be recorded? In other words, could subjects be recorded without knowing they are being recorded?		
Is it possible that any members of vulnerable populations (this could be any disadvantaged sub-segment of an overall population, e.g. children, prisoners, refugees, people facing discrimination) might be recorded?		

Use Face ID on your iPhone or iPad Pro

Face ID lets you securely unlock your iPhone or iPad, authenticate purchases, sign in to apps, and more — all with just a glance.



USD



Shop

Fusion PCB/PCBA

Community

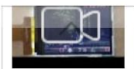
What are you looking for?



Sign in



Home / Development Platform / Programmer / MicroPython / Speed MAix BiT for RISC-V AI+IoT



Speed MAix BiT for RISC-V AI+IoT

SKU 102991150



3 Reviews



Speed newly provide breadboard-friendly board for you, it called MAix BiT. It integrate USB2UART chip, auto download circuit, RGB LED, DVP Camera FPC connector(support small FPC camera and standard M12 camera), MCU LCD FPC connector(support our 2.4 inch QVGA LCD), TF card slot.

\$12.90

110+ In Stock

2+: \$12.60

50+: \$12.20

- 1 +

CN Warehouse



Add to Cart



Chris Buck

@ChuBailiang

New York Times r
报驻华记者

Beijing

Joined Januar



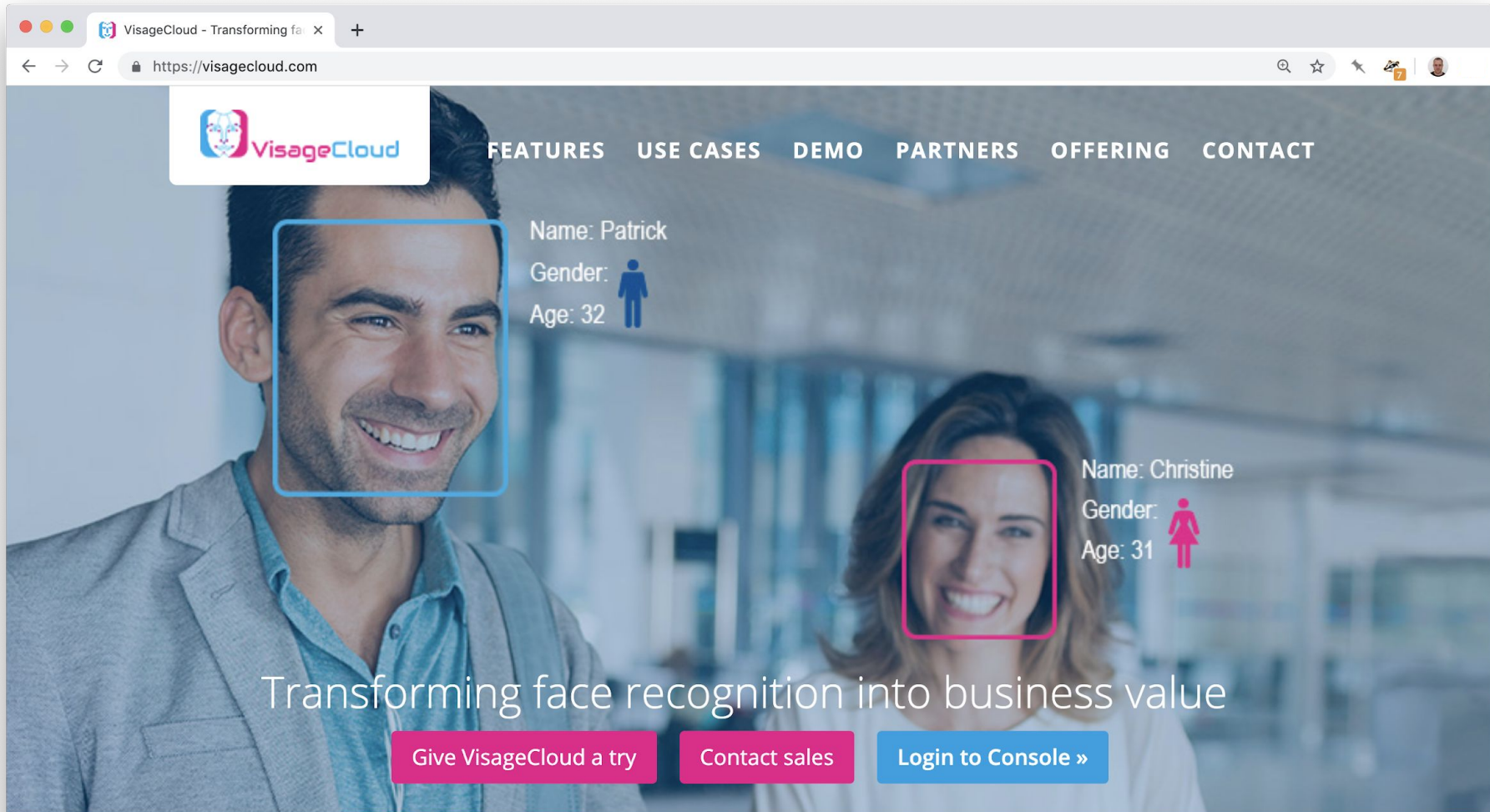
Chris Buckley 储百亮

@ChuBailiang

Following

Until I saw this picture, I never realized that face recognition technology for rationing toilet paper was so scary. goo.gl/Mcu4HZ







While designing the technical intricacies of deep learning and scaling our operations to tens and hundreds of thousands of faces, we always keep in mind the business challenges that our customers face. While excellence in user experience and technical performance often spearhead business objectives, compliance is a crucial part of success. One such challenge that we identified in the area of compliance is the approaching date of enforcement for the General Data Protection Regulation, the 25th of May 2018. The General Data Protection Regulation (GDPR) ([Regulation \(EU\) 2016/679](#)) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union. While the regulations set forth are of direct interest for businesses operating within the boundaries of the European Union, the GDPR establishes best practices for properly, securely and responsibly handling user/customer data in general.

For this reason we designed the technical aspects of VisageCloud by keeping in mind the data protection, control and security leverages needed to achieve GDPR compliance.

What does GDPR actually require?



[Browse](#) [Subscriptions](#) [Rankings](#) [Submit a paper](#) [My Library](#) [Blog](#)



[Create account](#)

[Sign in](#)

Not Available For Download

[★ Add Paper to My Library](#)

Share: [f](#) [t](#) [e](#) [s](#)

Consumer Rights Protection and Biometric Recognition Technology: An Unattainable Balance?

Posted: 17 Apr 2018

[Marta Santos Silva](#)

Maastricht University, Faculty of Law, Private Law Department

Date Written: April 1, 2018

Abstract

Biometric technology is part of our everyday connected lives. Wi-Fi tracking and radio waves, predicting analytics and deep learning allow its use for recognizing faces, voices, movements, personality and character. Governments and private companies have been applying biometric recognition technology in the sectors of fitness, healthcare, transportation, entertainment and security. More recently, the retail marketing industry has been resorting to it to monitor and control consumer engagement levels in real time thereby generating new sources of income. Biometric technology is unobtrusive, and it can be used to provide more impressive, tailor-made experiences to consumers. However, the intrusiveness of this technology, readily accessible in mobile phone's front cameras, as well as the immutability of the datasets and the impossibility of anonymising them through differential privacy techniques, or of replacing them in case of hacking, gives room for serious concern. Recognition technology poses critical threats to privacy and civil liberties, such as free association and free expression. From another perspective, this disruption also threatens to affect

Register to save articles to your library

[Register](#)

Paper statistics

ABSTRACT VIEWS

260

PlumX Metrics



Related eJournals

Ethics eJournal

[Follow](#)

[Feedback](#)

GENERAL DATA PROTECTION REGULATION (GDPR)

RECITALS

KEY ISSUES

Deutsch

Chapter 1 (Art. 1 – 4)

General provisions

Chapter 2 (Art. 5 – 11)

Principles

Art. 5 – Principles relating to processing of personal data

Art. 6 – Lawfulness of processing

Art. 7 – Conditions for consent

Art. 8 – Conditions applicable to child's consent in relation to information society services

Art. 9 – Processing of special categories of personal data

Art. 10 – Processing of personal data relating to criminal convictions and offences

Art. 11 – Processing which does not require identification

Chapter 3 (Art. 12 – 23)

Rights of the data subject

Chapter 4 (Art. 24 – 43)

Controller and processor

Chapter 5 (Art. 44 – 50)

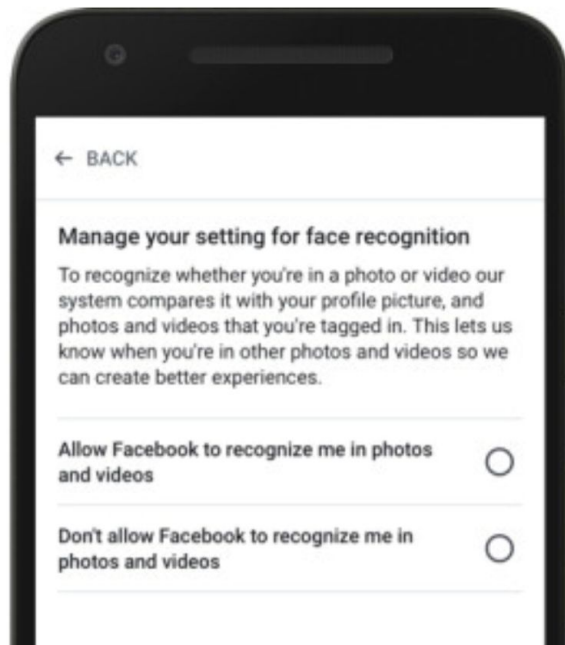
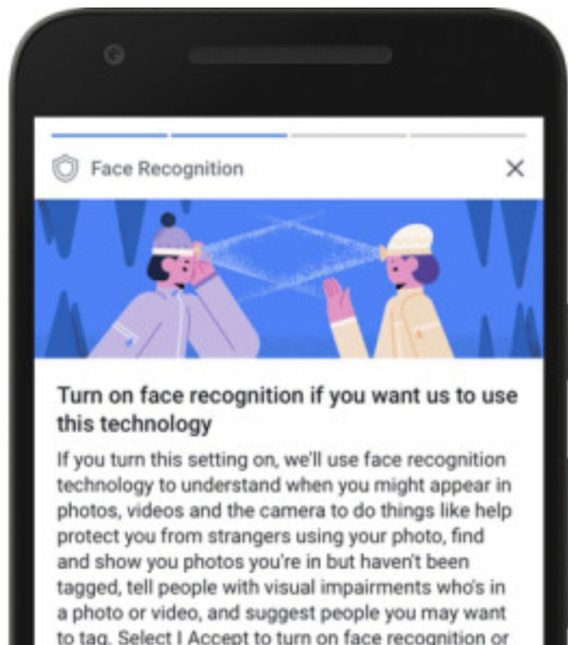
Transfers of personal data to third countries or international organisations

Art. 7 GDPR


Conditions for consent

- Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
- ¹ If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. ² Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
- ¹ The data subject shall have the right to withdraw his or her consent at any time. ² The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. ³ Prior to giving consent, the data subject shall be informed thereof. ⁴ It shall be as easy to withdraw as to give consent.
- When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

For instance, here's Facebook's FRT opt-in page for Europe and Canada...



Home



Matthew Brennan
@mbrennanchina

China Tech | Speaker
Tencent specialist
media inquiries: info@mbrennanchina.com

People's Republic of China



Matthew Brennan

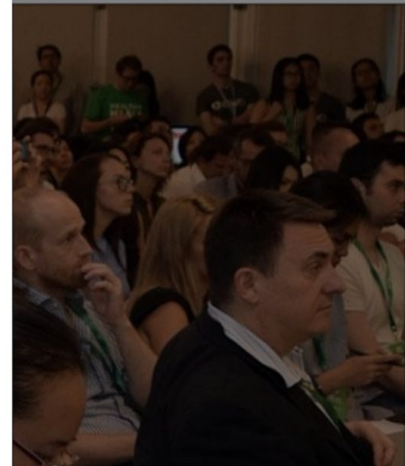
@mbrennanchina

Follow

Wow! China Airport face recognition systems to help you check your flight status and find the way to your gate. Note I did not input anything, it accurately identified my full flight information from my face!



Tweet



Assisting Users in a World Full of Cameras

A Privacy-aware Infrastructure for Computer Vision Applications

Anupam Das, Martin Degeling, Xiaoyou Wang, Junjue Wang, Norman Sadeh, Mahadev Satyanarayanan
Carnegie Mellon Univeristy

{

Abstract

Computer vision based technologies have seen widespread adoption over the recent years. This use is not limited to the rapid adoption of facial recognition technology but extends to facial expression recognition, scene recognition and more. These developments raise privacy concerns and call for novel solutions to ensure adequate user awareness, and ideally, control over the resulting collection and use of potentially sensitive data. While cameras have become ubiquitous, most of the time users are not even aware of their presence. In this paper we introduce a novel distributed privacy infrastructure for the Internet-of-Things and discuss in particular how it can help enhance user's awareness of and control over the collection and use of video data about them. The

these cameras create, process and transfer personally identifiable information to an extent that often remains unknown to those being affected by the technology. Therefore regulators are now investigating particular applications of computer vision [52] and there is a growing need for tools that inform users about what data is collected and what choices they have with respect to how the data is used.

In this paper, we focus on the use of facial recognition because this technology has not only improved in accuracy and performance that surpasses human performance in certain cases [52], but also seen wide spread adoption and steady growth in the commercial sector [4]. By definition facial recognition refers to a biometric technology that identifies individuals based on their distinctive and measurable facial patterns. Traditionally, facial recognition technology has been utilized by government and law enforce-

Our PEP maintains a database for storing each user's privacy settings, e.g., to disable facial recognition during specific times of the day or when one is at a specific location.

6. Privacy-aware Video Streaming

We integrate our privacy-aware notification infrastructure with a video denaturing system to build a privacy-aware video streaming service. Our proposed system informs users of nearby cameras when they approach the vicinity of deployed cameras. It also provides users with an opt-in choice (as our default policy is opt-out) to facial recognition based services. We have developed an *automated class attendance* app as one possible application. Other use cases where facial recognition technology best fits our infrastructure include automated menu suggestion, admission to transportation systems or checkout kiosks. In the following section we will first briefly describe the different components of the face denaturing system. Next, we will describe the interactions that take place among the different components. Lastly, we present some performance and scalability results. The face denaturing system proposed by Wang et al. [54] consists of a *Face Trainer* and a *Privacy*

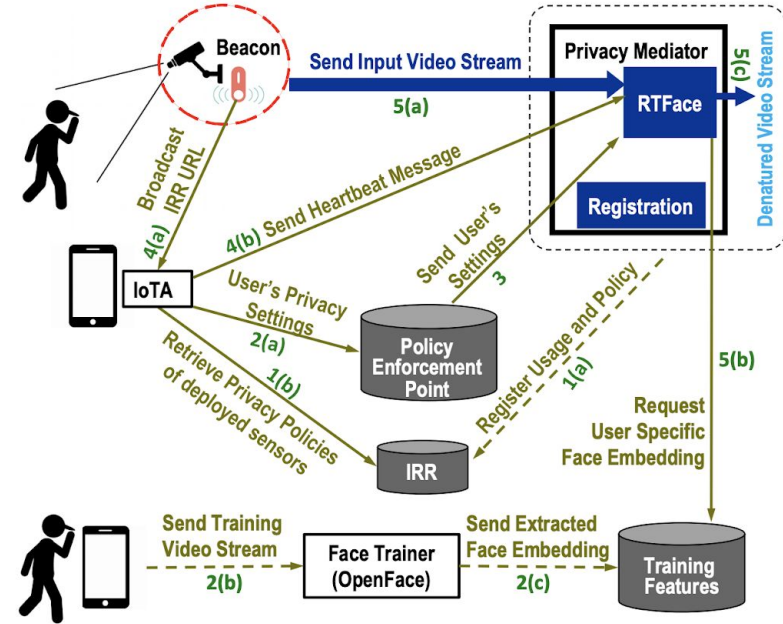


Figure 3: Privacy-aware video streaming infrastructure. Numbers in the figure correspond to the different steps in the overall work flow.

used to perform facial recognition in her vicinity. She can review the privacy policy associated with the technology and decide, e.g., on whether or not she wants to support the purpose for which the data is collected. The IoT also shows to her that a service called 'Auto

Home



Dennis Crowley

@dens

Follow

Great read. ps: It just dawned on me that those "check-in for your flight w/ your face!" airport cameras may be designed to generate more "name-to-face" training data for all the other facial recognition algorithms.



Opinion | San Francisco Is Right: Facial Recognition Must Be Put On ...

The technology is unregulated and rife with error. We shouldn't deploy it without strong privacy rules.

Dennis Cro

@dens

I like to build thing

@StockadeFC

Husband to @

& . I enjoy s

hot dogs

Tweet

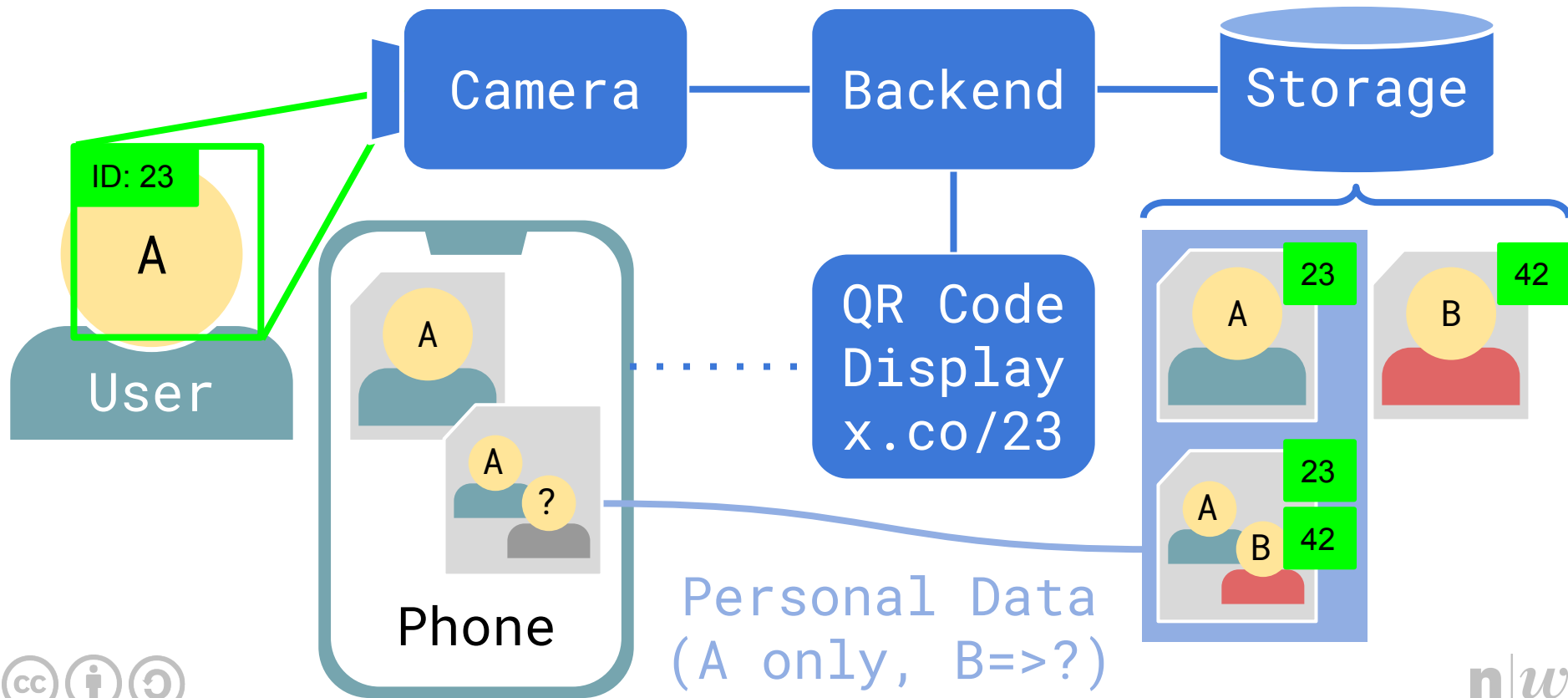




The right to view your data

You can access your
personal data free of charge.

Reclaiming data with your face



Good Practices for Capability URLs

W3C Draft TAG Finding 30 October 2018



Latest editor's draft:

<https://w3ctag.github.io/capability-urls/>

Editor:

Jeni Tennison ([ODI](#))

Repository:

[We are on Github.](#)

[File a bug.](#)

[Commit history.](#)

Copyright © 2018 [W3C](#)[®] ([MIT](#), [ERCIM](#), [Keio](#), [Beihang](#)). W3C [liability](#), [trademark](#) and [permissive document license](#) rules apply.

Abstract

Capability URLs grant access to a resource to anyone who has the URL. There are particular application design patterns for which this is useful as they remove the necessity for users to log in to a site and are easily delegated



Search



How Good Is Facebook's Facial Recognition?

660,745 views

7.3K

430

SHARE

SAVE

