

**Was die  
Technologie von  
der Politik lernen  
muss**



# Zentralisierte Daten

## Ein Alptraum für den Datenschutz

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
>	Fenway Community Health Center, Inc.	MA	Healthcare Provider	598	11/29/2023	Unauthorized Access/Disclosure	Paper/Films
>	Lakeview Healthcare System, LLC	FL	Healthcare Provider	2495	11/27/2023	Theft	Paper/Films
>	Molina Healthcare of Iowa, Inc.	IA	Business Associate	1647	11/22/2023	Hacking/IT Incident	Email
>	Saisystems International, Inc.	CT	Business Associate	10063	11/22/2023	Hacking/IT Incident	Network Server
>	The Charles Lea Center	SC	Healthcare Provider	1250	11/22/2023	Hacking/IT Incident	Network Server
>	Northwest Eye Care Professionals	OR	Healthcare Provider	950	11/22/2023	Hacking/IT Incident	Network Server
>	TGI Direct, Inc.	MI	Business Associate	16113	11/21/2023	Hacking/IT Incident	Network Server
>	Detroit Chassis, LLC	MI	Health Plan	958	11/21/2023	Hacking/IT Incident	Network Server
>	Proliance Surgeons	WA	Healthcare Provider	437392	11/20/2023	Hacking/IT Incident	Network Server

Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Summe der bisher betroffenen Personen im Jahr 2023:

**111,907,232**

# Zentralisierte Daten

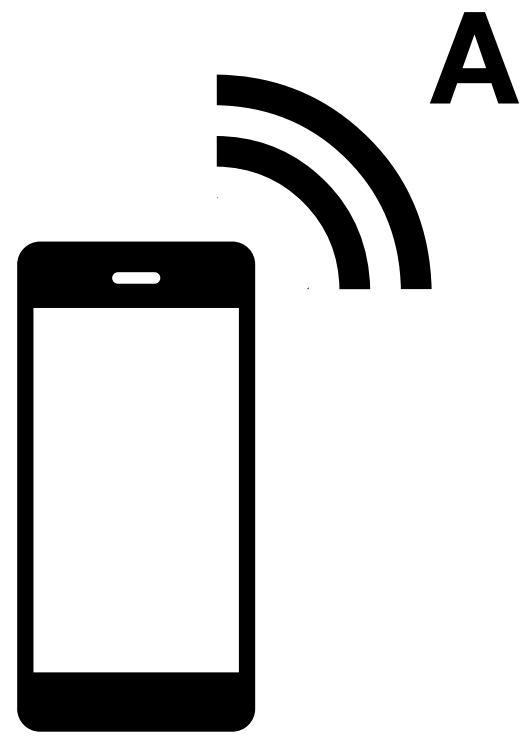
## Eine falsche Wahl

- + “Datenschutz ODER Bekämpfung der Pandemie”
- + “Datenschutz ODER gute Digitalisierung”
- + “Datenschutz ODER Künstliche Intelligenz”
- + Das sind immer falsche Wahlmöglichkeiten.

**EPFL**

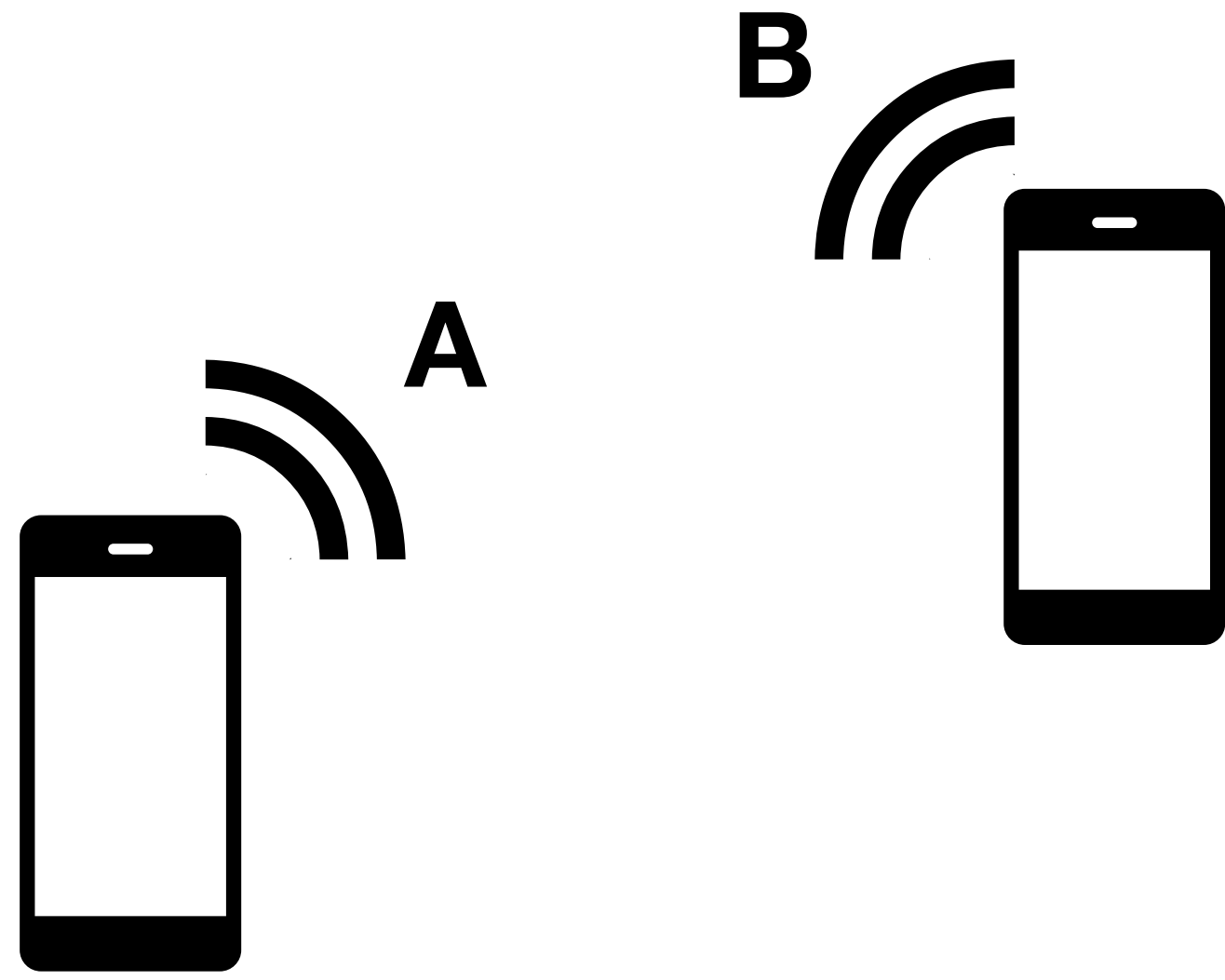
**COVID-19**

# **Digital Proximity Tracing**



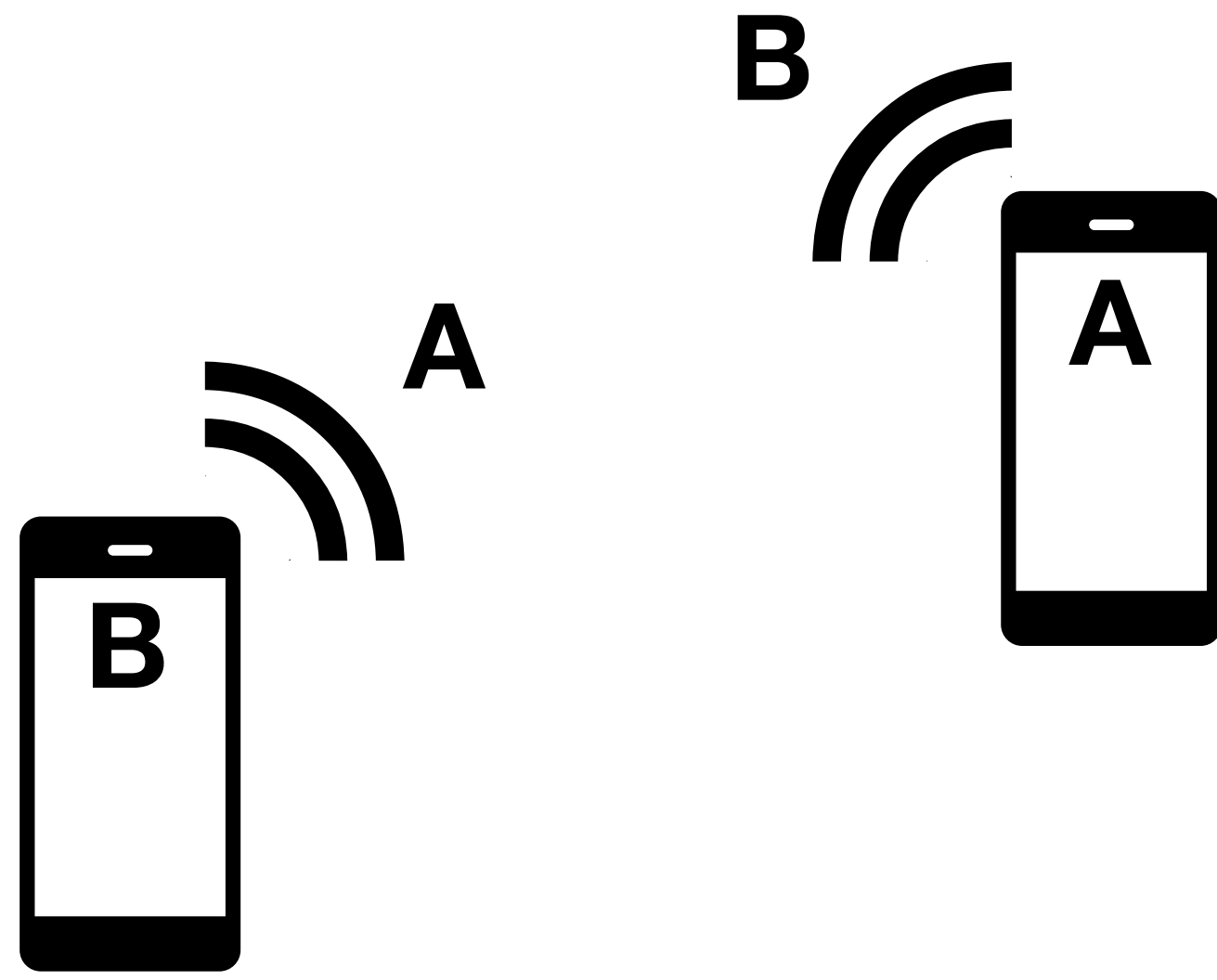


# Digital Proximity Tracing





## Digital Proximity Tracing

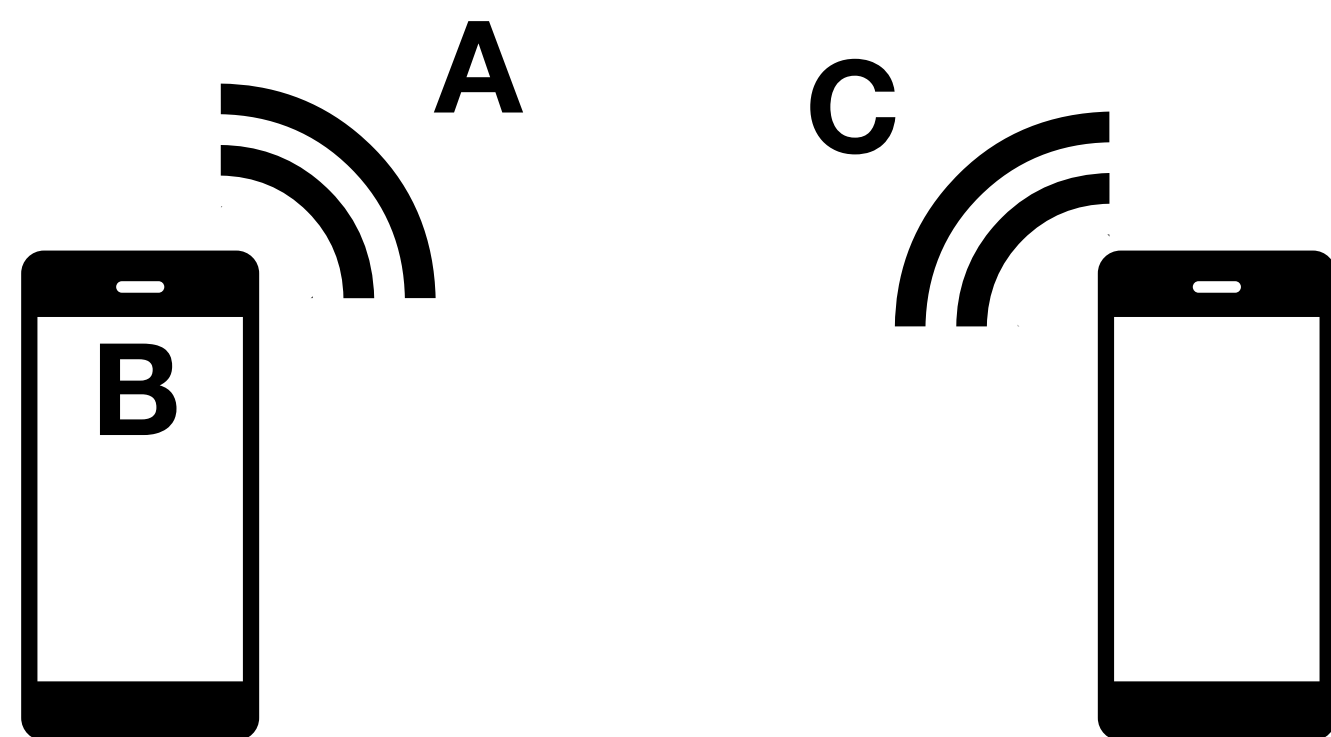




**EPFL**

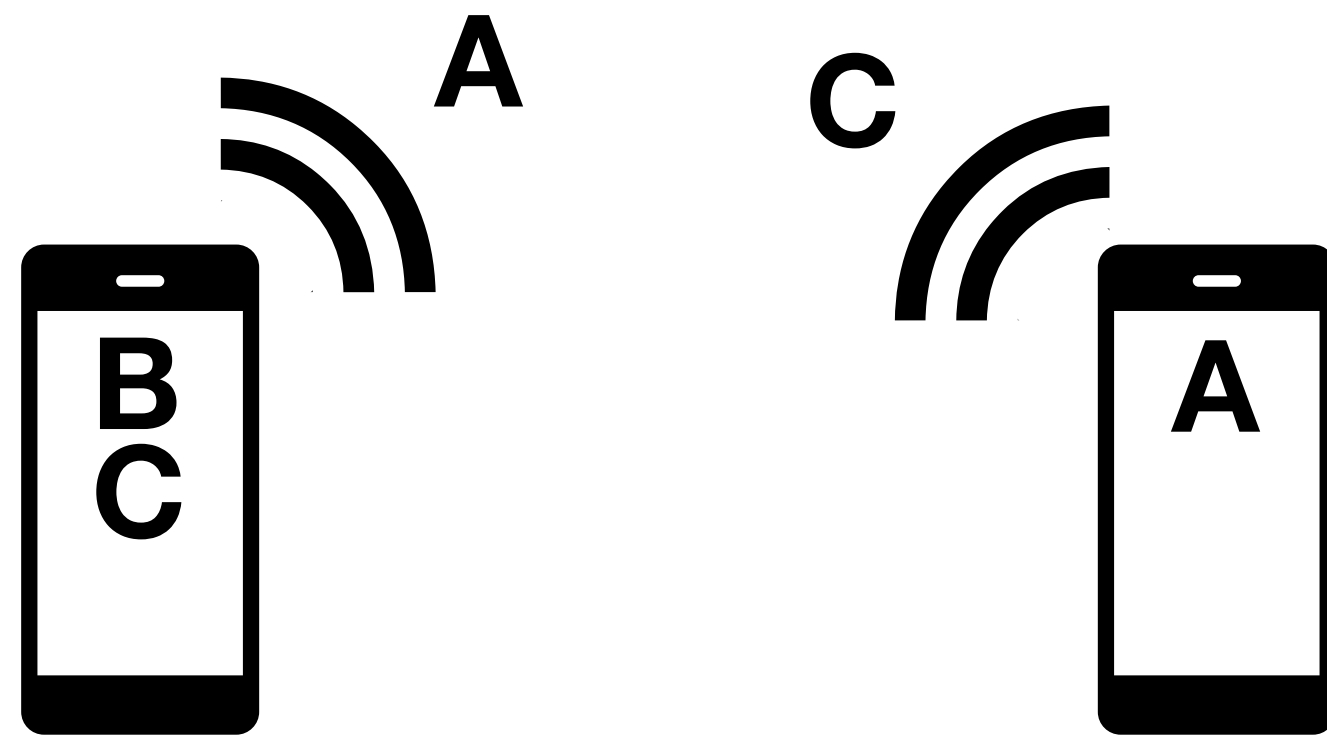
**COVID-19**

# **Digital Proximity Tracing**





## Digital Proximity Tracing

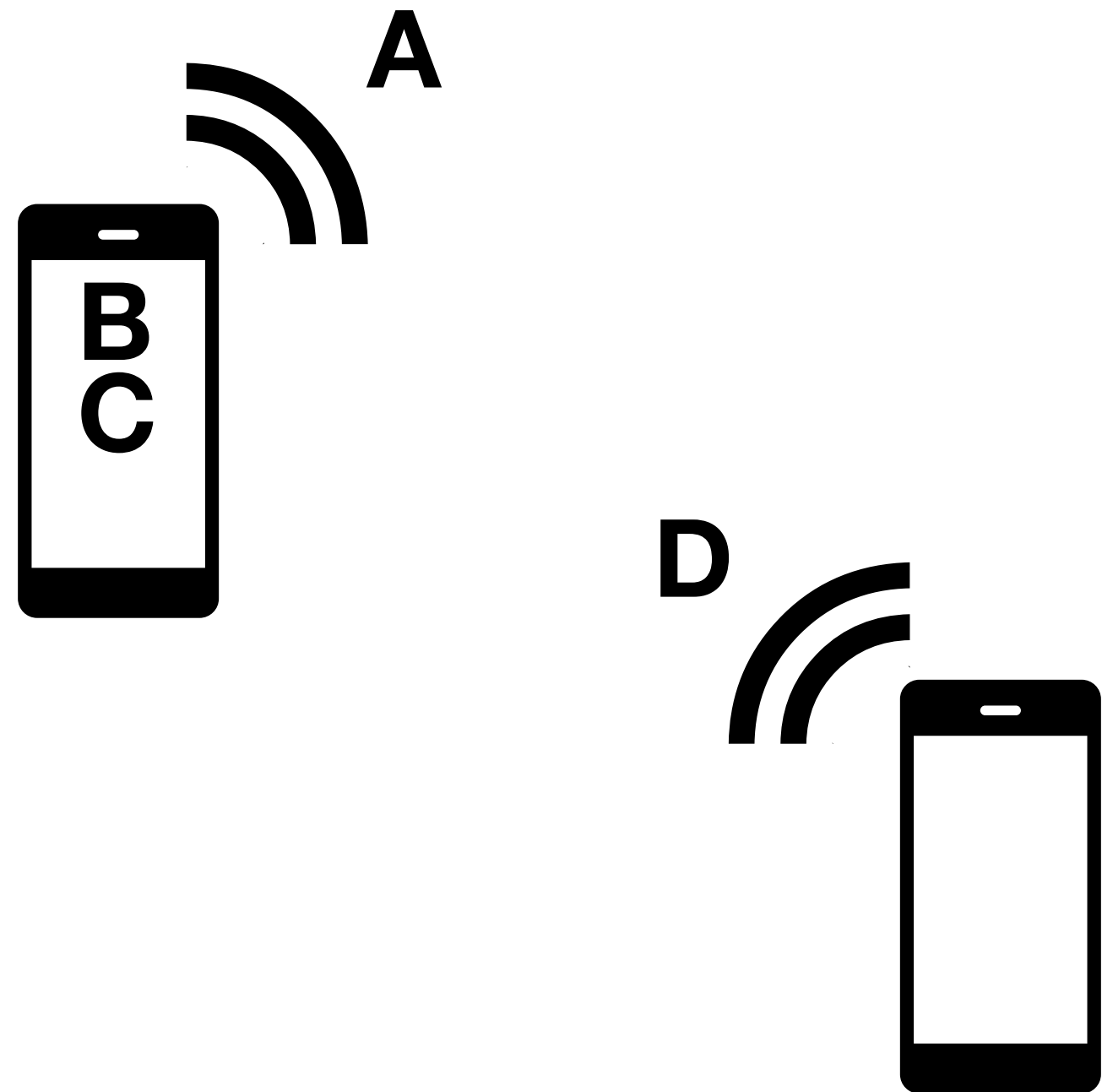




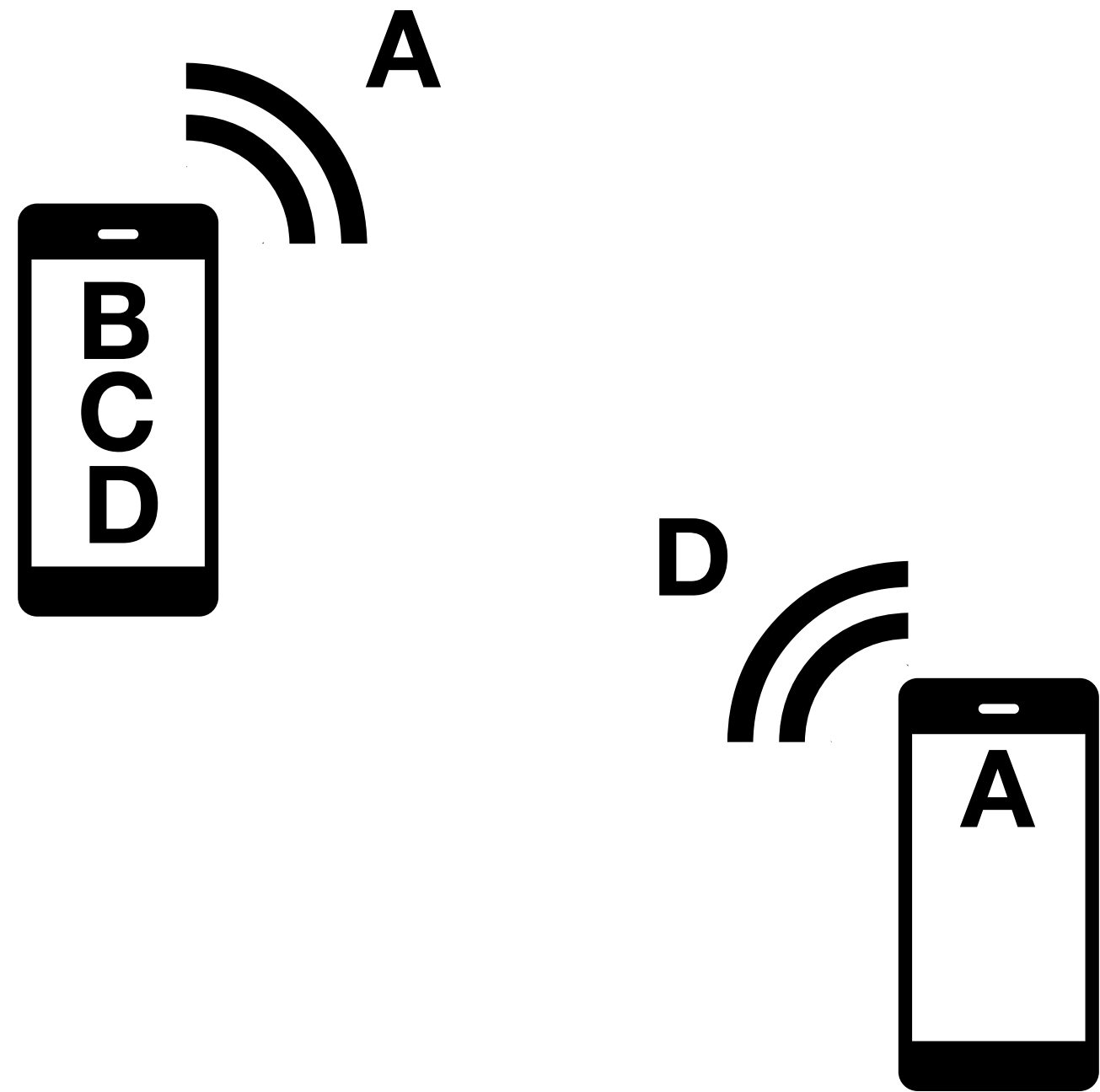
**EPFL**

**COVID-19**

# **Digital Proximity Tracing**

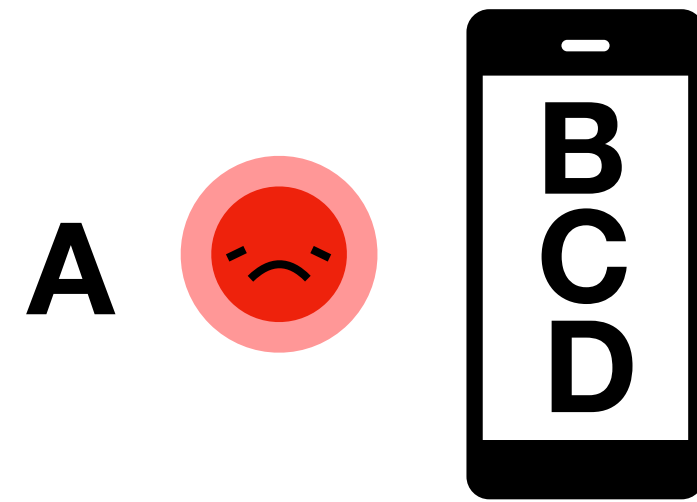


## Digital Proximity Tracing

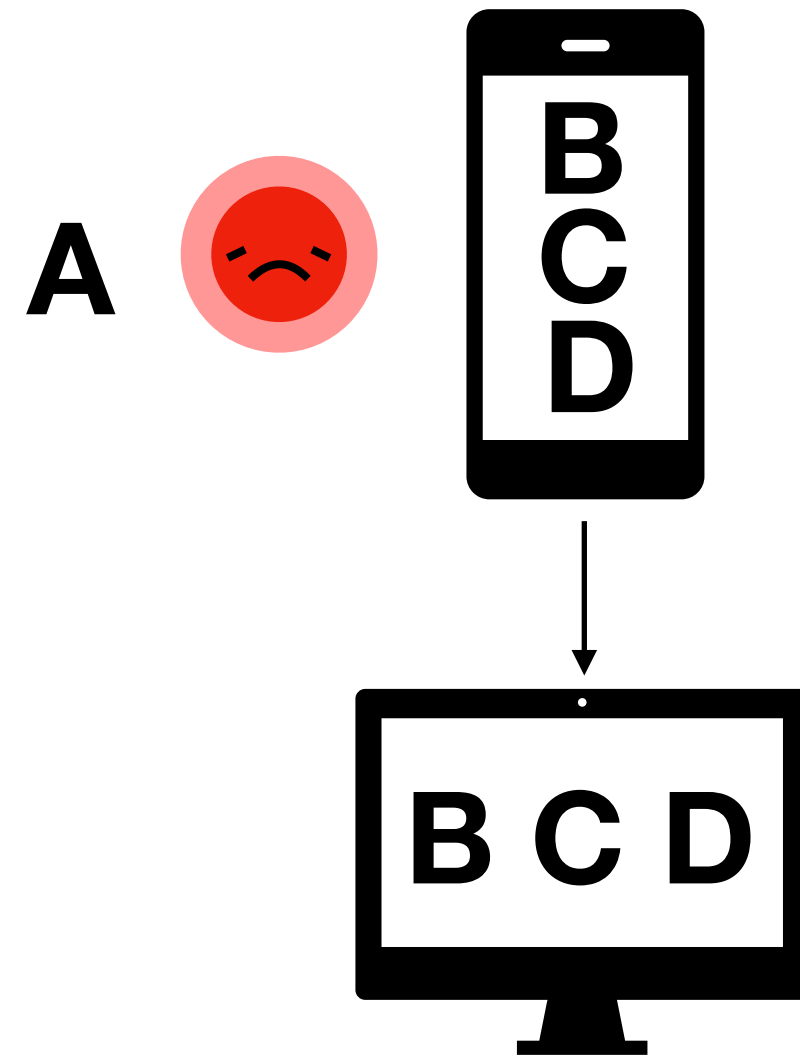




## Zentralisiertes Model

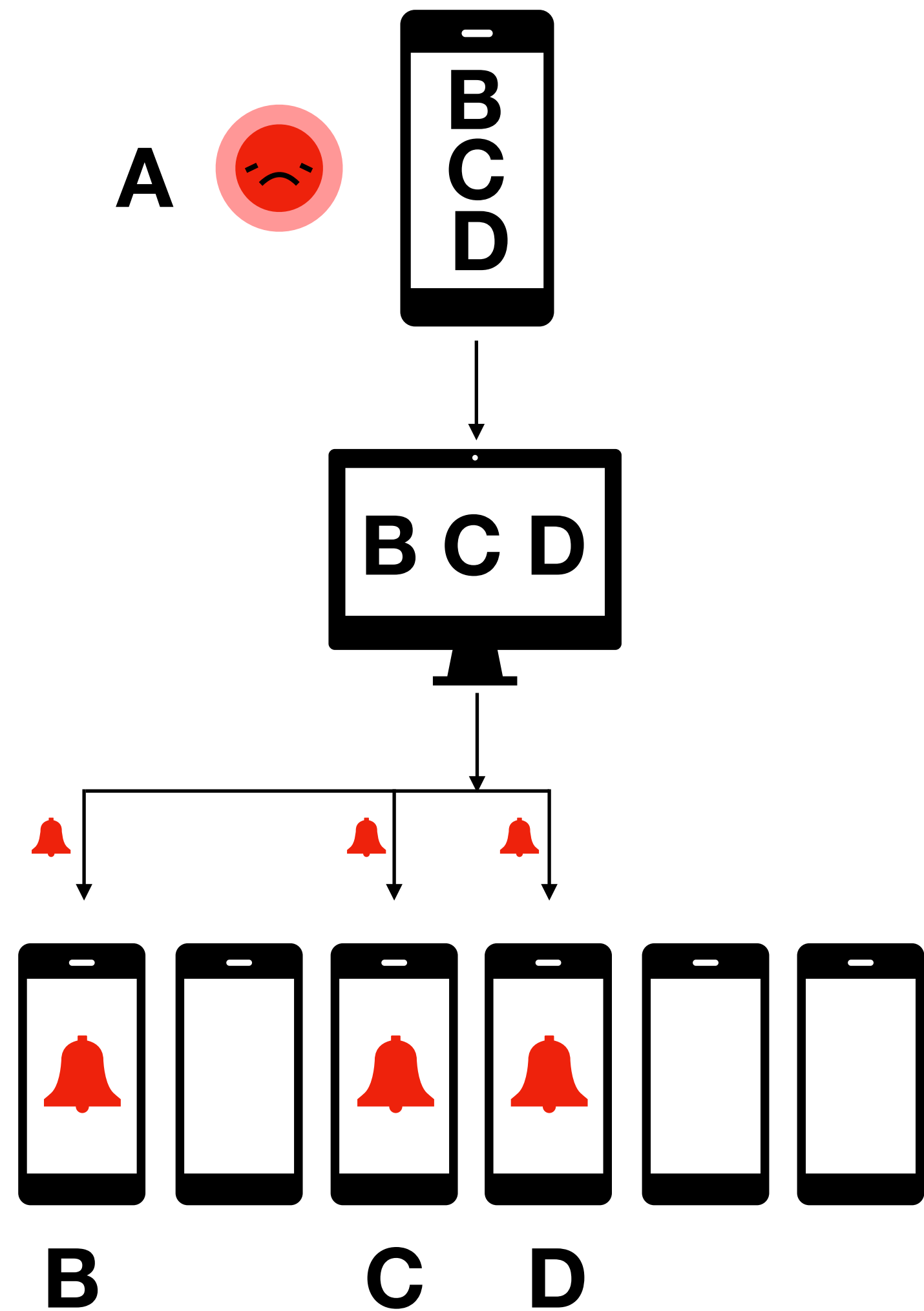


## Zentralisiertes Model

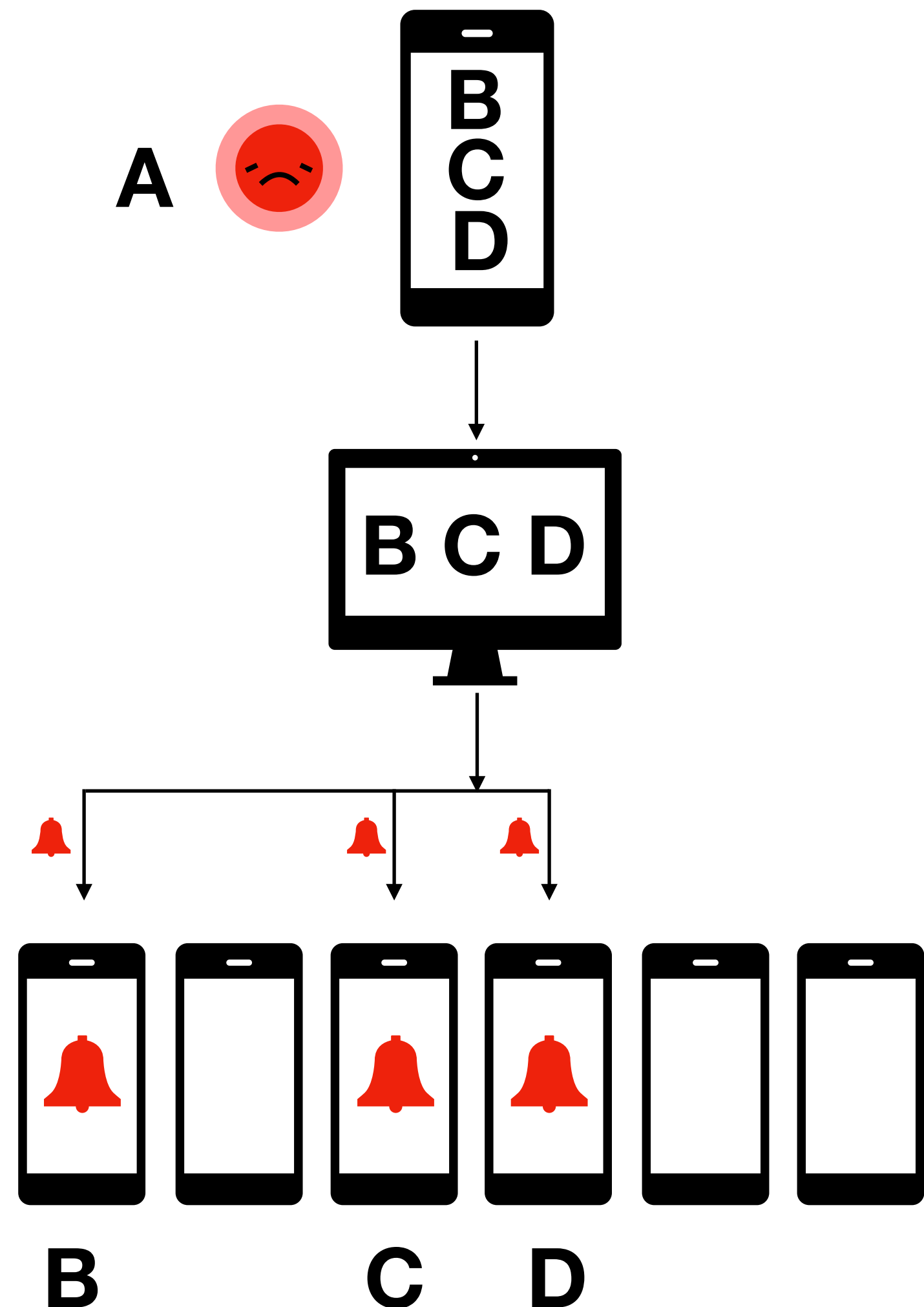




## Zentralisiertes Model



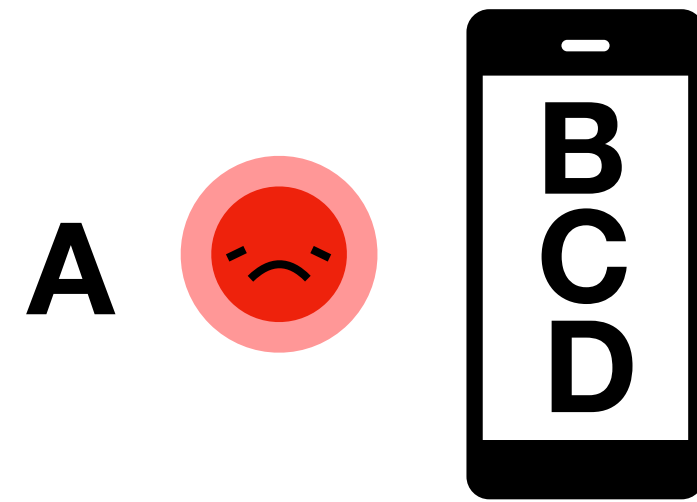
# Zentralisiertes Model



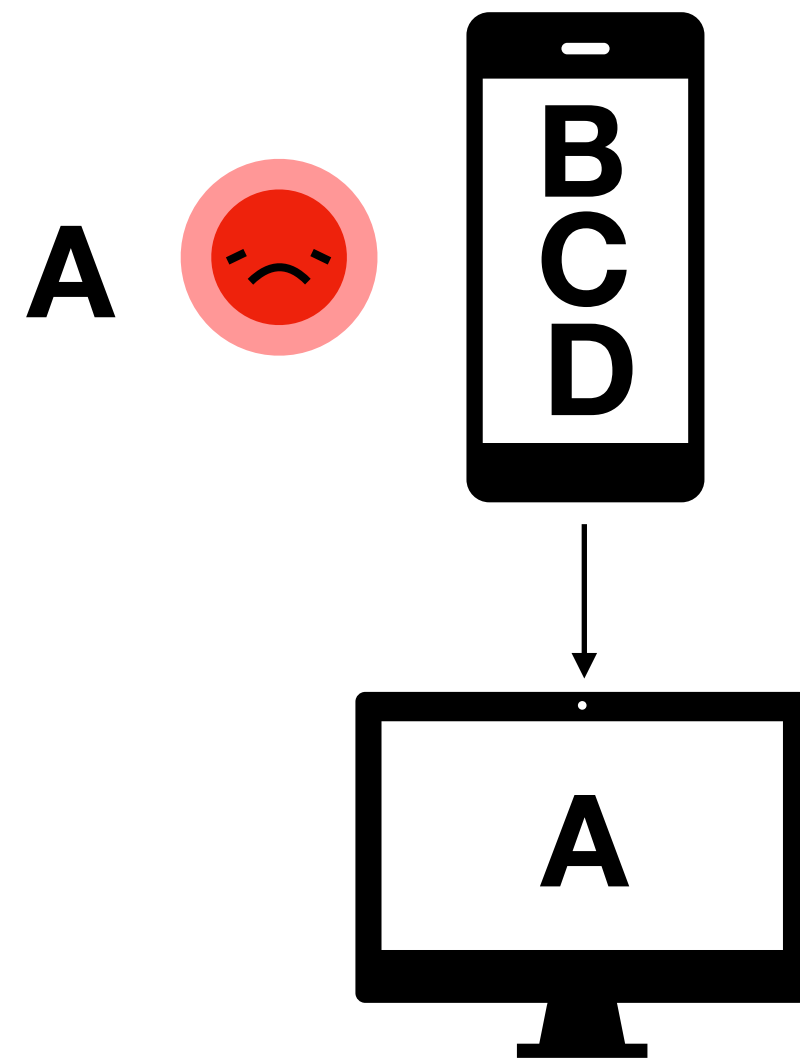
- + Der zentrale Server weiss jetzt, dass B, C und D mit jemand anderem Kontakt hatten.
- + Mit der Zeit könnten Kontaktnetze abgeleitet und die Daten für andere Zwecke verwendet werden.
- + Nutzer verlieren die Kontrolle über die Daten



## Dezentralisiertes Model

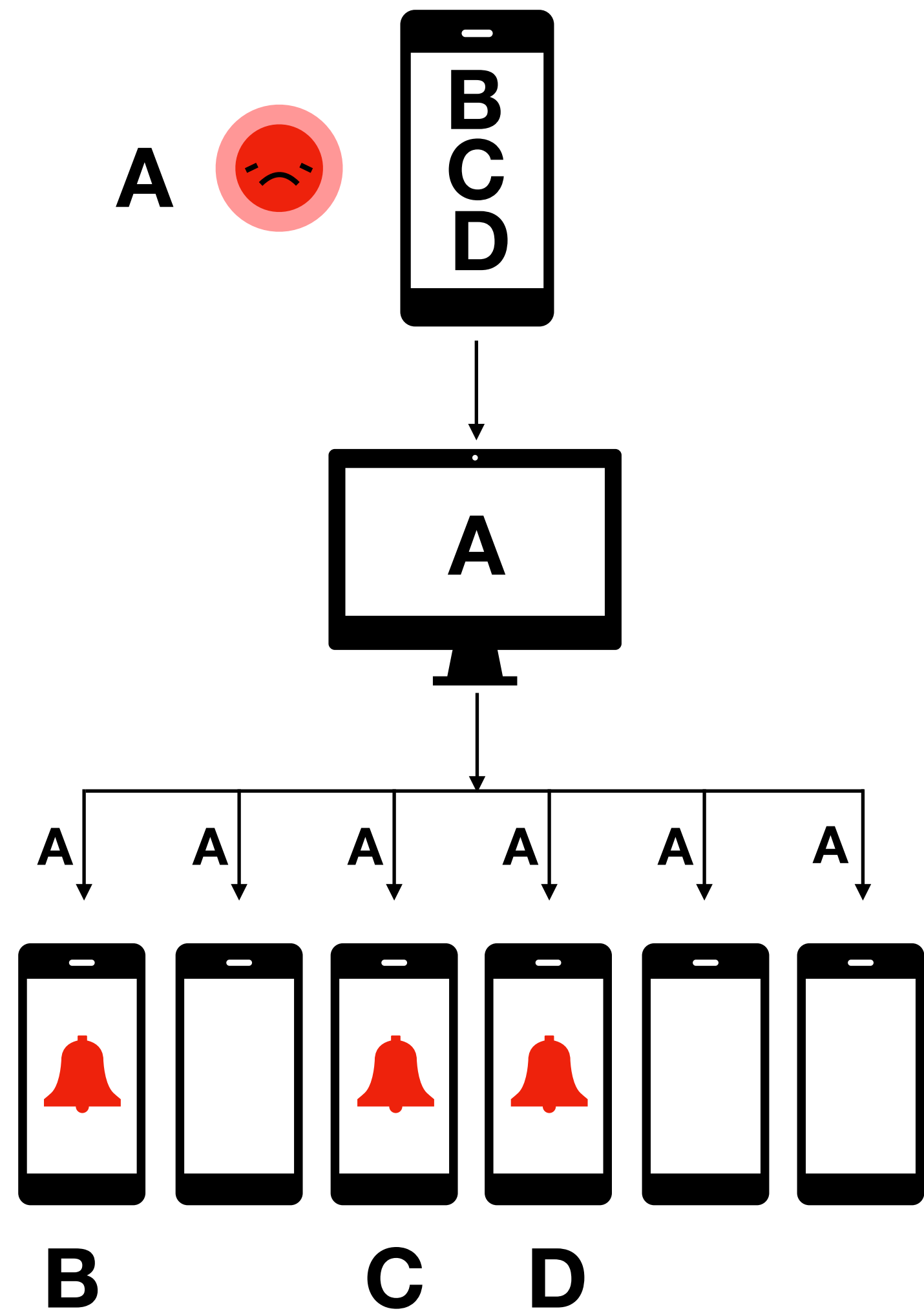


## Dezentralisiertes Model

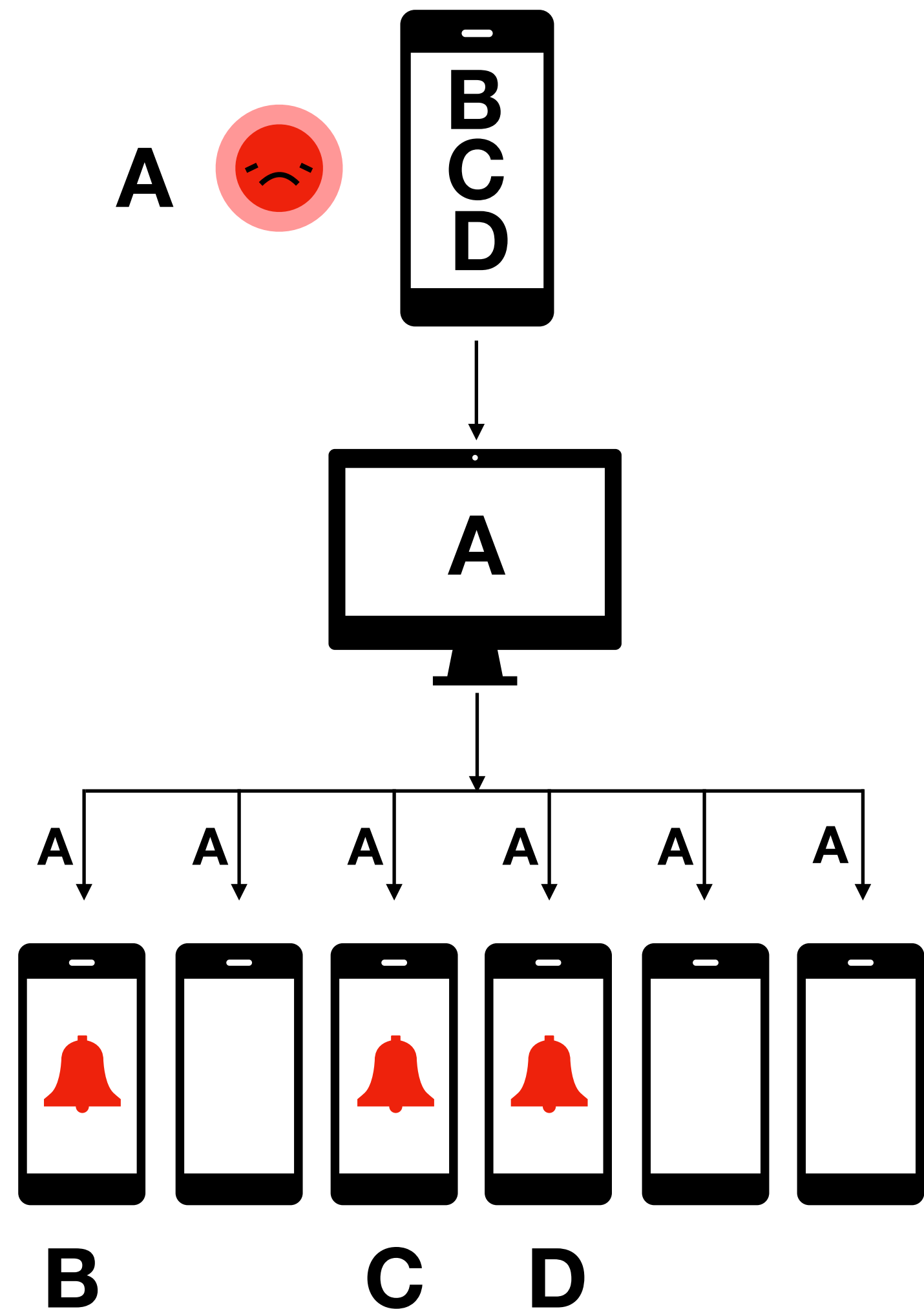




## Dezentralisiertes Model



# Dezentralisiertes Model



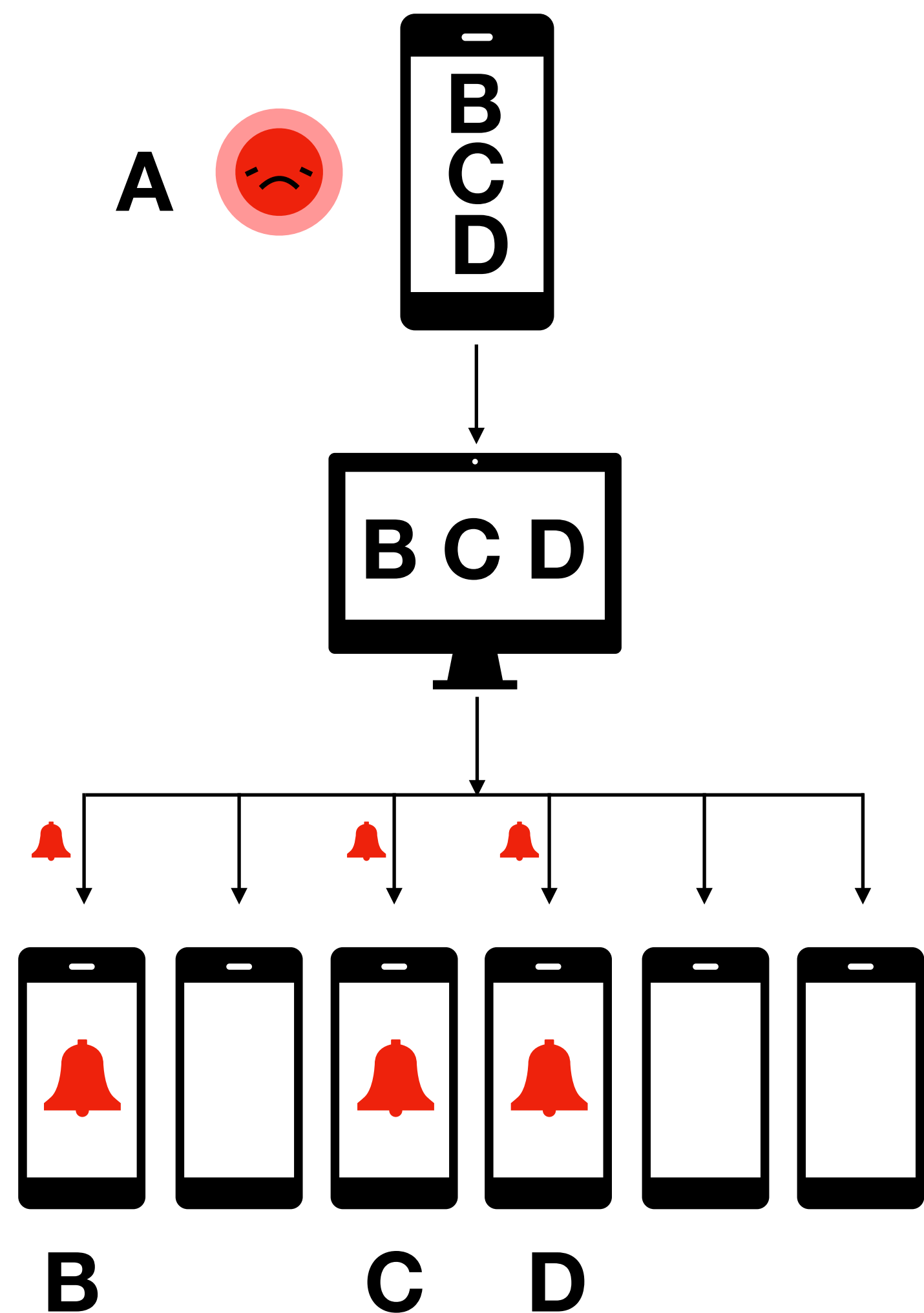
- + Sensitive Kontaktdaten bleiben auf dem Gerät
- + Die Entscheidung über die Benachrichtigung wird *lokal* getroffen, nicht auf einem zentralen Server
- + Server weiss nur, welche IDs *infiziert* wurden

**EPFL**

**COVID-19**

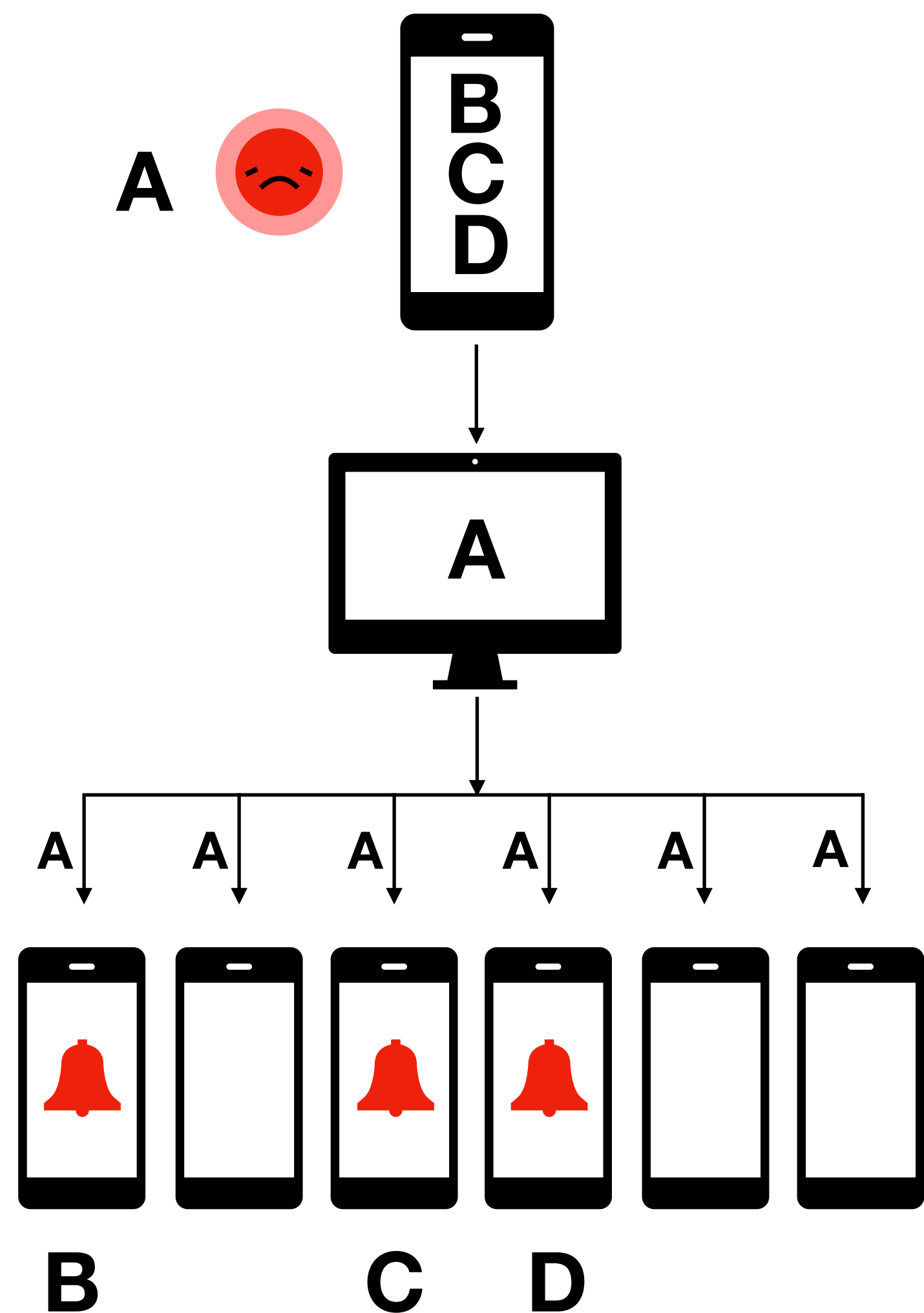
**Anderer Prozess, gleiches Resultat**

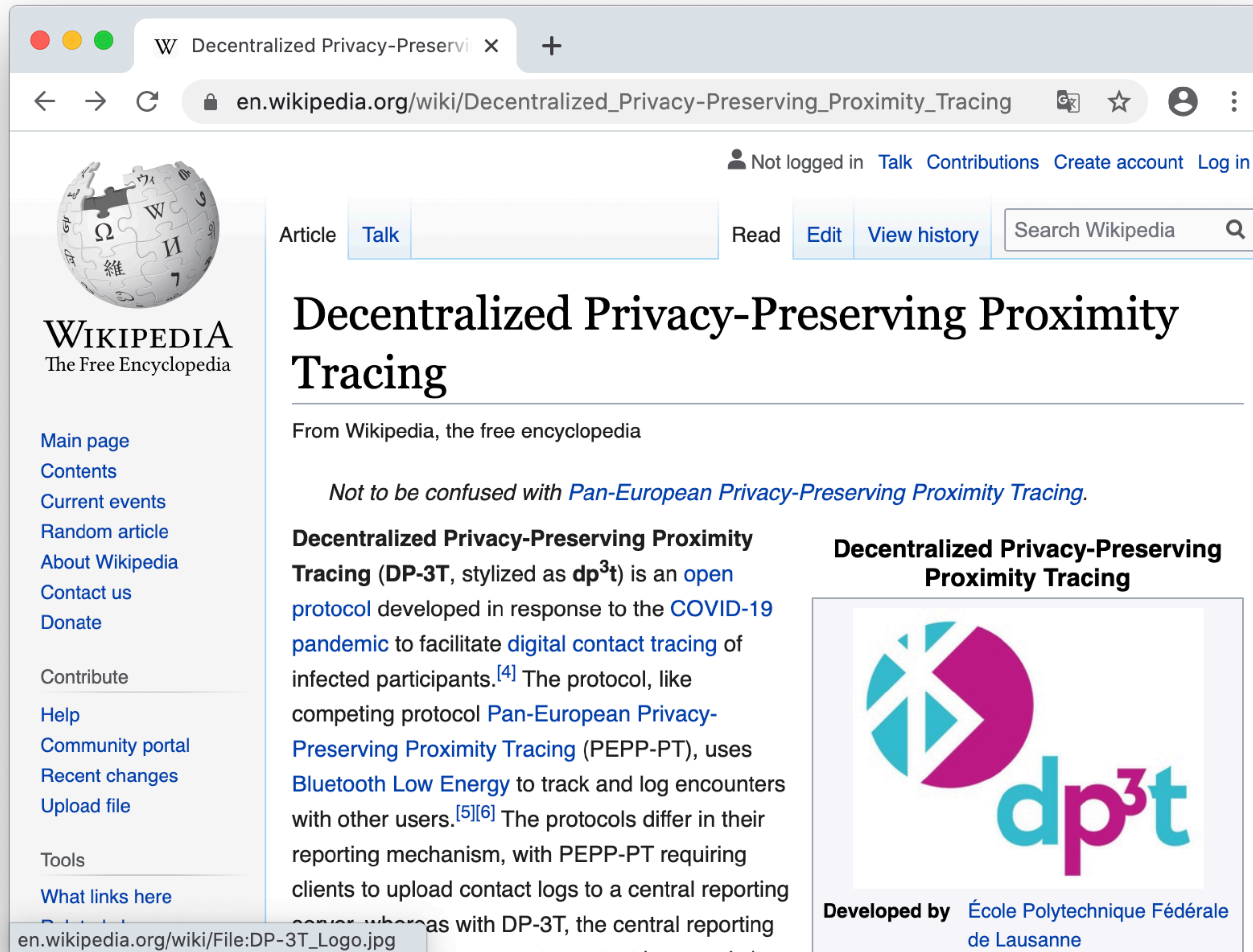
## Anderer Prozess, gleiches Resultat



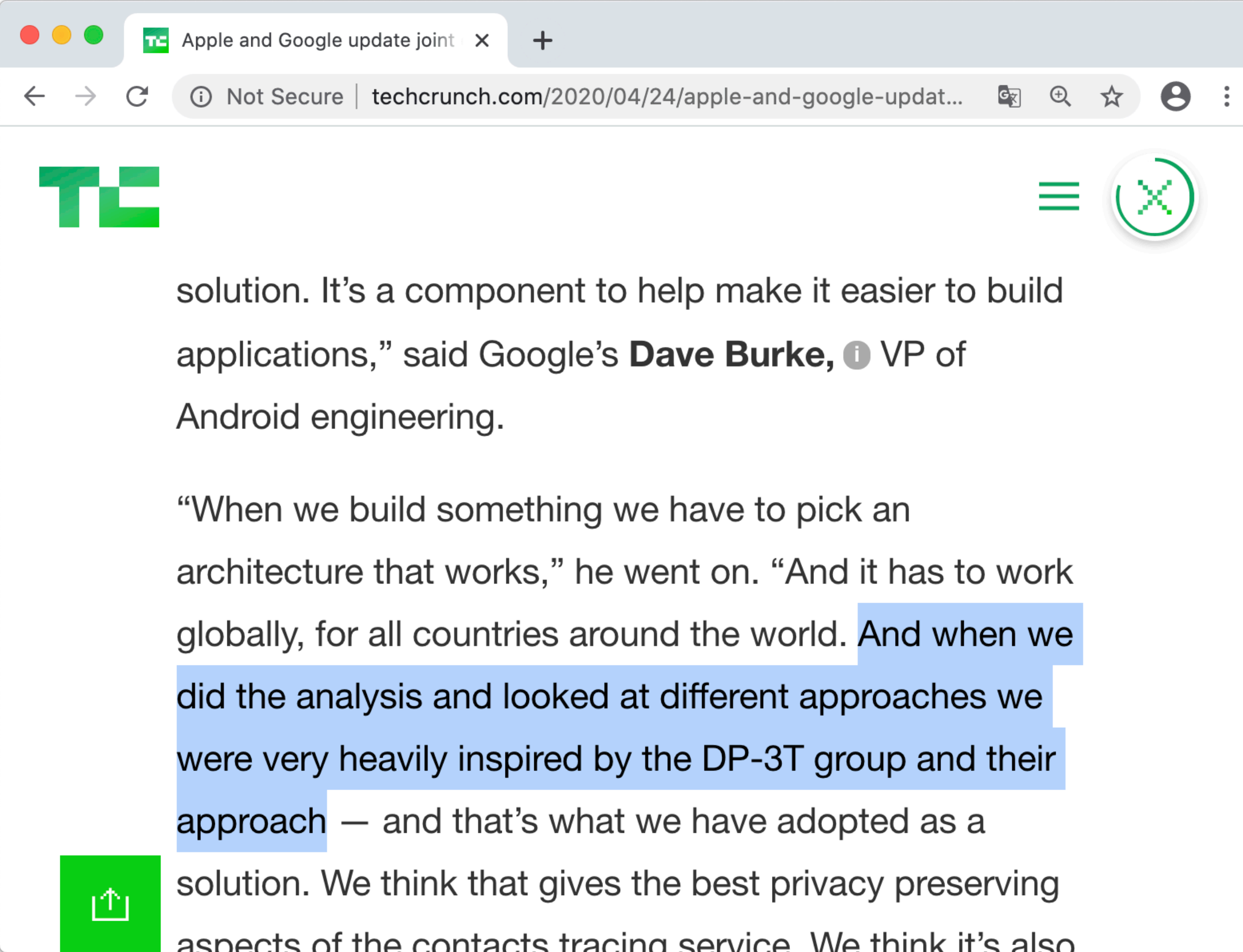


## Anderer Prozess, gleiches Resultat





The screenshot shows a web browser window displaying the Wikipedia article for "Decentralized Privacy-Preserving Proximity Tracing". The browser's address bar shows the URL: `en.wikipedia.org/wiki/Decentralized_Privacy-Preserving_Proximity_Tracing`. The page header includes the Wikipedia logo and navigation links such as "Not logged in", "Talk", "Contributions", "Create account", and "Log in". The article title is prominently displayed, followed by the text "From Wikipedia, the free encyclopedia". A note states: "Not to be confused with *Pan-European Privacy-Preserving Proximity Tracing*." The main text begins with: "Decentralized Privacy-Preserving Proximity Tracing (DP-3T, stylized as **dp<sup>3</sup>t**) is an open protocol developed in response to the COVID-19 pandemic to facilitate digital contact tracing of infected participants.<sup>[4]</sup> The protocol, like competing protocol Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), uses Bluetooth Low Energy to track and log encounters with other users.<sup>[5][6]</sup> The protocols differ in their reporting mechanism, with PEPP-PT requiring clients to upload contact logs to a central reporting server, whereas with DP-3T, the central reporting" (text is partially cut off). To the right, there is a section titled "Decentralized Privacy-Preserving Proximity Tracing" featuring the logo for dp<sup>3</sup>t, which consists of a stylized 'd' and 'p' in teal and purple, and '3t' in teal. Below the logo, it says "Developed by École Polytechnique Fédérale de Lausanne". A sidebar on the left contains various Wikipedia navigation links. A small tooltip at the bottom left shows the file path: `en.wikipedia.org/wiki/File:DP-3T_Logo.jpg`.



The image shows a screenshot of a web browser displaying a TechCrunch article. The browser's address bar shows the URL: `techcrunch.com/2020/04/24/apple-and-google-updat...`. The article text is partially visible, with several lines highlighted in blue. A green share icon is visible in the bottom left corner of the article content area.

Apple and Google update joint

Not Secure | techcrunch.com/2020/04/24/apple-and-google-updat...

TC

solution. It's a component to help make it easier to build applications," said Google's **Dave Burke**, VP of Android engineering.

"When we build something we have to pick an architecture that works," he went on. "And it has to work globally, for all countries around the world. And when we did the analysis and looked at different approaches we were very heavily inspired by the DP-3T group and their approach — and that's what we have adopted as a solution. We think that gives the best privacy preserving aspects of the contacts tracing service. We think it's also

# **Es gab zentrale Apps**

- + Jeder einzelne Fall von Missbrauch/Datenverlust betraf zentralisierte Anwendungen.

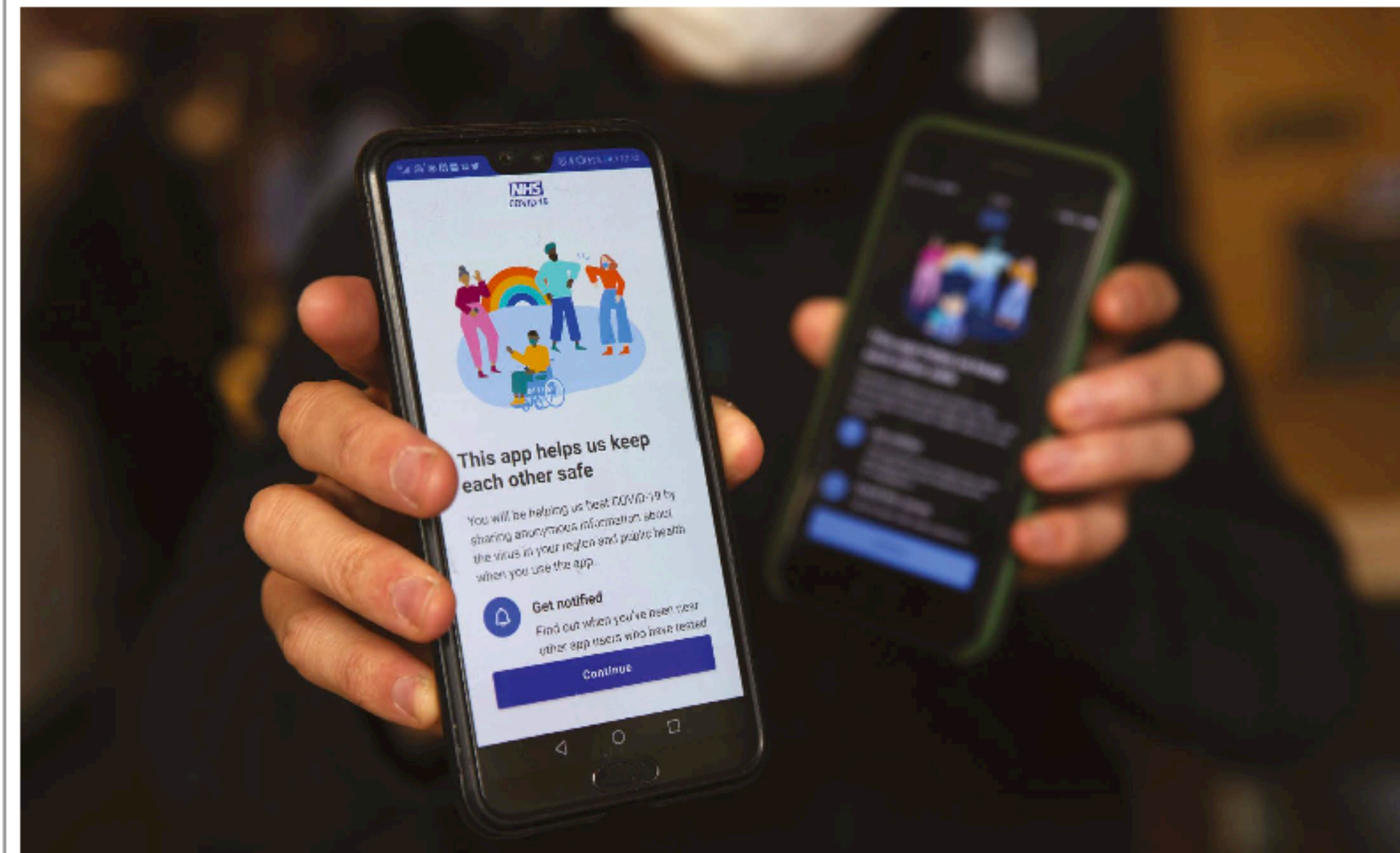


# Dezentralisierte Apps waren sicher

- + Es gab keinen einzigen Datenmissbrauch oder Datenverlust, **da dies praktisch unmöglich war.**



# Comment



The National Health Service launched a digital contact-tracing app for COVID-19 in England and Wales in September 2020.

## Privacy-preserving contact tracing curbed COVID

Marcel Salathé

Despite controversies over decentralized contact-tracing apps, the data now show that they saved thousands of lives during the pandemic. National and international authorities must heed the lessons.

**D**uring the first year of the COVID-19 pandemic, around 50 countries deployed digital contact tracing. When someone tested positive for SARS-CoV-2, anyone who had been in close proximity to that person (usually for 15 minutes or more) would be notified as long as both individuals had installed the contact-tracing app on their devices.

Digital contact tracing received much media attention, and much criticism, in that first year. Many worried that the technology provided a way for governments and technology companies to have even more control over people's lives than they already do. Others dismissed the apps as a failure, after public-health

authorities hit problems in deploying them.

Three years on, the data tell a different story. The United Kingdom successfully integrated a digital contact-tracing app with other public-health programmes and interventions, and collected data to assess the app's effectiveness. Several analyses now show that, even with the challenges of introducing a new technology during an emergency, and despite relatively low uptake, the app saved thousands of lives. It has also become clearer that many of the problems encountered elsewhere were not to do with the technology itself, but with integrating a twenty-first-century technology into what are largely twentieth-century public-health infrastructures.

## Comment

Today, national and international health authorities are not investing in digital contact tracing. Nor are they including it in pandemic-preparedness plans (see, for example, [go.nature.com/434gvja](https://go.nature.com/434gvja)). Even the announcement of a major digital health initiative, launched by the World Health Organization (WHO) and the European Commission last month to "protect citizens across the world from on-going and future health threats" failed to mention it (see [go.nature.com/3ckypcg](https://go.nature.com/3ckypcg)). This misses a crucial opportunity to prevent future outbreaks from escalating into pandemics.

To harness this potentially transformative tool in future, policymakers and other stakeholders must heed the evidence – and the lessons – now emerging from its use during the COVID-19 pandemic.

### Privacy, please

In March 2020, it became clear that the speed of SARS-CoV-2 transmission would outpace conventional contact tracing<sup>1</sup>, which generally involves public-health workers interviewing people known to have contracted the virus and then reaching out to identified contacts to ask them to get tested or go into quarantine. Stuck at home, scientists and engineers worldwide – myself included – began to collaborate remotely on how to implement digital contact tracing at scale.

At the time, health authorities in many countries were envisioning a centralized system. Many of the people I spoke to argued that having a database under government control would be crucial to ascertain whether the approach was working, and to improving it. They often seemed unaware of the potential privacy implications of a centralized database. (These became clearer later, for instance, when the Singapore authorities admitted that data from a centralized digital contact-tracing system, called TraceTogether, could also be accessed by the police, contrary to previous assurances.) In the media, too, a narrative seemed to be emerging that in the face of a historic pandemic, privacy concerns would have to take a back seat.

To some of us, however, the perceived conflict between curbing the disease and protecting privacy was a mirage. We set out to develop a decentralized system that would notify people of whether they had been exposed to COVID-19, without letting central actors gather massive databases of highly sensitive information. One of these systems was the DP3T protocol<sup>2</sup>, which I helped to develop at the Swiss Federal Institute of Technology in Lausanne (EPFL), along with engineers, computer scientists and legal experts at other universities.

Instead of gathering contact information on central servers, the DP3T protocol, which we made publicly available on GitHub on 3 April 2020, kept it safely on people's smartphones.

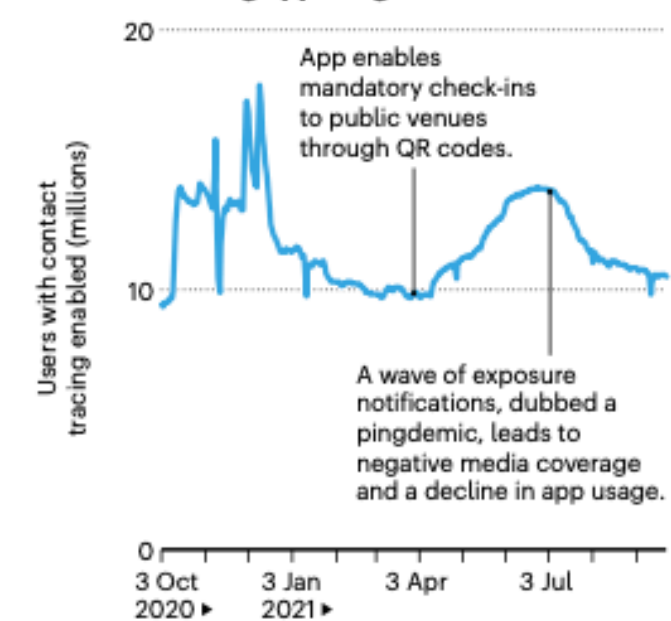
Any decision about notifying someone would be made by an app on the phone, rather than a central server. In other words, the protocol ensured that people would get notified without governments having access to information on their contacts<sup>3</sup>.

On 10 April 2020, Google and Apple, the providers of the world's two dominant mobile operating systems, announced their release of

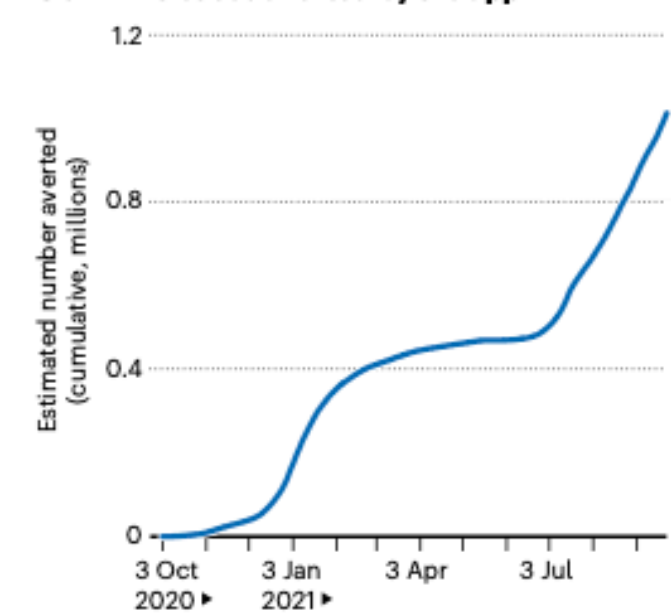
### WHAT THE DATA SAY

Digital contact tracing saved thousands of lives during the COVID-19 pandemic in England and Wales – where the app was integrated with other public-health interventions and continually improved by the National Health Service.

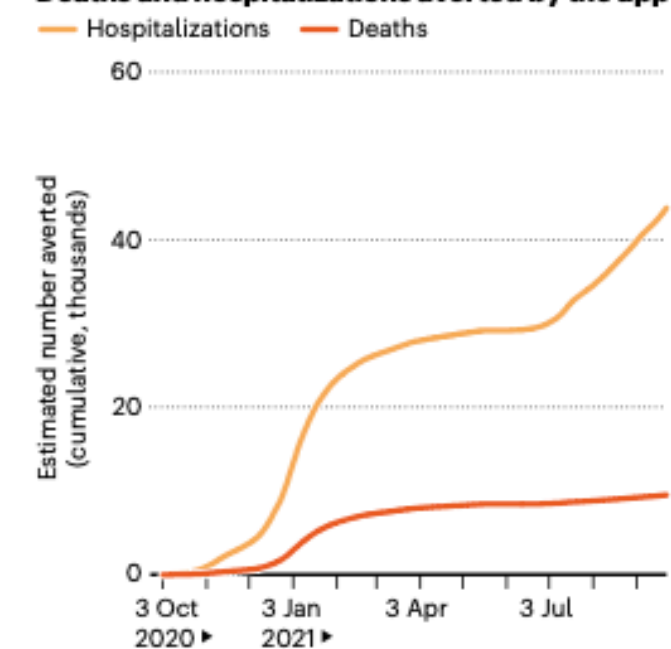
#### Contact-tracing app usage



#### COVID-19 cases averted by the app



#### Deaths and hospitalizations averted by the app



'Exposure Notification' technology – essentially a variant of the DP3T protocol. Public-health agencies would now be able to incorporate it into their own contact-tracing apps.

At this time, I was having frequent virtual meetings with health officials from many countries, or their scientific advisers. It was clear that Google's and Apple's insistence on privacy-preserving contact-tracing apps frustrated governments around the world. At the time, many health authorities planning to roll out digital contact tracing pleaded with the tech giants to reconsider their stance. But eventually, most of them began to deploy the Exposure Notification protocol.

The second wave of COVID-19 hit soon after the apps using this technology were being introduced in mid-2020, in countries such as Switzerland, Germany, Italy and Latvia. Amid a lull in cases beforehand, and mounting media criticism of the apps, public-health authorities struggled to integrate them into their health-care systems – and to convince the public to use them<sup>4</sup>. When COVID-19 surged in the Northern Hemisphere in autumn, digital contact tracing often fell by the wayside while governments focused on health-care provision.

Many countries had already been struggling to keep up with the demand for COVID-19 testing. In countries such as Switzerland and Finland<sup>5</sup>, health authorities now also struggled to keep up with demand for app activation codes. The delays frustrated users and undermined the main purpose of digital contact tracing: to deliver information at speed<sup>6</sup>. Thus, the perception grew globally that the apps were a failure.

Although it is easier, in principle, to assess the effectiveness of digital contact tracing when it is centralized, there are ways to do this for decentralized versions, too<sup>7,8</sup>. Instead of relying on centralized data collection, analysts can use questionnaires or approaches such as telemetry to map how many notifications were made and where, how many of these happened on phones that also reported a positive test result and so on. All of this can be done without revealing the identities of the people whose phones were receiving the alerts.

Few countries gathered these data during the chaos of the first year of the pandemic, but the United Kingdom did. A study conducted during the first three months of the UK National Health Service's (NHS's) deployment of a decentralized contact-tracing app – the NHS COVID-19 app for England and Wales – showed that the app could trace more than twice as many contacts as could conventional contact tracing<sup>9</sup>. Two analysis methods were used: one using modelling and the other a statistical approach. These estimated that, in just three months, the app prevented 284,000 or 594,000 cases, respectively – despite only 28% of the population in those regions using it. The study also suggested that for every 1% increment in app usage, the



A health worker comforts a person in an inten...

number of cases could be reduced by 0.8% and 2.3%, respectively.

The most compelling evidence yet, however, comes from an analysis published earlier this year of the usage and impact of the NHS COVID-19 app in its first year of deployment<sup>10</sup>. It found that the app prevented around one million infections and saved more than 9,600 lives in England and Wales between September 2020 and September 2021. And it achieved this even though, on average over the year, only around 25% of the population was using it (see 'What the data say').

### Invest now

In April this year, the WHO launched an initiative to improve preparedness for pandemics and other emerging threats (see [go.nature.com/3nn8rd5](https://go.nature.com/3nn8rd5)). In my view, the WHO should strongly advise countries to adopt privacy-protecting digital contact tracing. The WHO is also well positioned to develop guidance on evaluating digital contact tracing. Such guidance can build on initiatives during the COVID-19 pandemic, such as the 'indicator framework'<sup>11</sup> of the WHO and the European Centre for Disease Control and Prevention, which provides countries with a standardized approach for this evaluation.

The WHO is not yet a leading actor in digital health, and a separate organization should be created to focus on further developing digital contact-tracing technology, in collaboration with the companies that control mobile operating systems. A diversity of players would need to be involved – specialists in

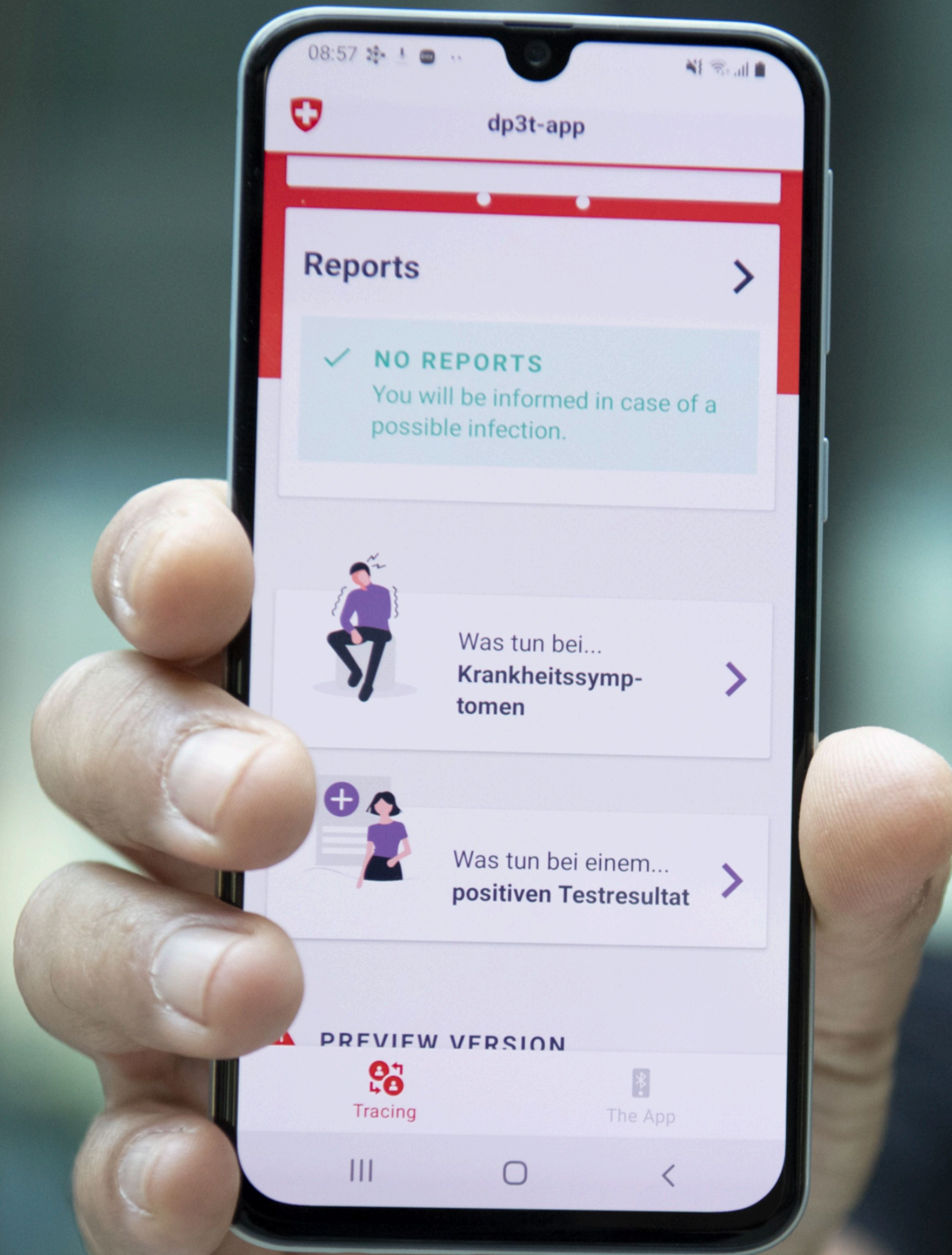


# Was wir lernen können

## Dezentralität

- + Dezentralität ist in unserer DNA
- + Dezentralität verhindert Machtmissbrauch
- + Dezentralität ermöglicht Datenschutz
  
- + Dezentralität ist etwas komplizierter und langsamer
- + Dezentralität kostet etwas mehr
  
- + Zentrale Koordination wird essentiell





**Was die  
Technologie von  
der Politik lernen  
muss**