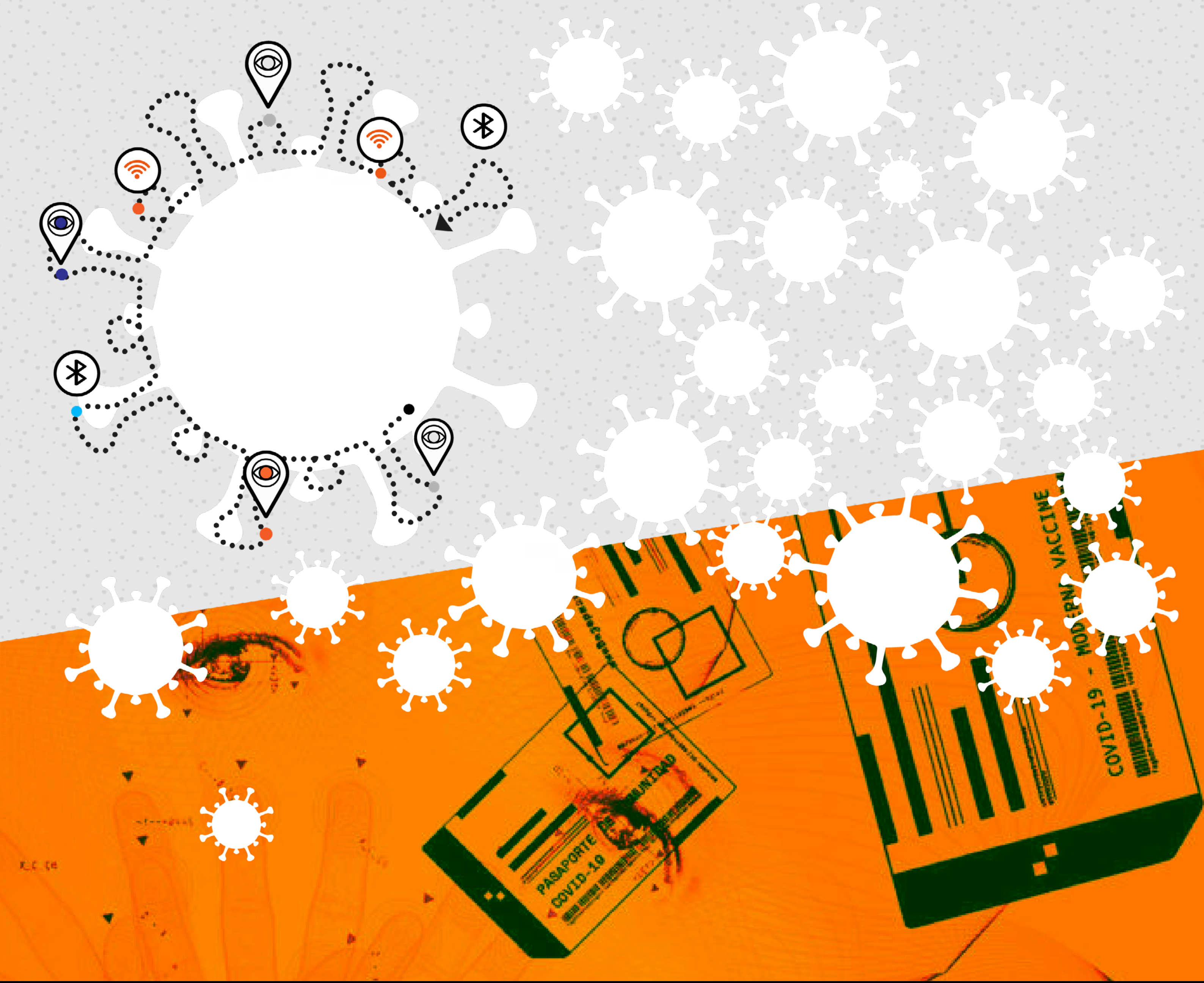
ONE YEAR UNDER COVID-19 CONTACT TRACING APPS: WHAT HAS EUROPE LEARNED?

#trackthetrackers



CIVIL
LIBERTIES
UNION FOR
EUROPE

accessnow

Publisher

Civil Liberties Union for Europe e.V
Ringbahnstraße 16-18-20
12099 Berlin, Germany
www.liberties.eu

Author

Estelle Massé (Access Now)
Orsolya Reich (Civil Liberties Union for Europe)
Eva Simon (Civil Liberties Union for Europe)

The Digital Freedom Fund's COVID-19 Litigation Fund allowed research on contact tracing apps to be conducted in twelve EU Member States for the purposes of deciding over possible future strategic litigation actions and allowed Access Now and Civil Liberties Union for Europe to analyse Europe's technological response to the pandemic.

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Table of contents

Introduction

Governments are under the obligation to protect the health, lives, and livelihoods of people in their jurisdiction. After the first few weeks of the 2020 spring lockdown(s) in Europe, nearly all European Union Member State governments decided to launch contact-tracing mobile phone applications. It was hoped that the widespread use of such apps would allow governments to limit the spread of the virus while making it possible for people and businesses to return to normal life.

The COVID-19 pandemic has been the first global pandemic where personal technological devices are well-spread and "smart" enough to make mass surveillance of the population through their own devices possible. As human rights defenders, we have been highly concerned that -- at least some -- European governments may introduce technological solutions that allow for technologies used as a response to the COVID-19 crisis to be repurposed for mass surveillance, and that these solutions may become permanent features in our daily lives. These concerns were exacerbated by the fact that democracy and the rule of law are steeply declining in a number of EU Member States.

Thankfully, the worst-case scenarios have not materialised so far. This is due in part thanks to the efforts and engagement of privacy experts in the design of COVID-19 tools (in particular the developers of the so-called DP-3T protocol[1]) but also, to a degree, thanks to the (unverified) privacy commitments made by tech giants Google and Apple, who took over the development of the infrastructure behind most national apps. Over the last year, contact tracing apps, to the best of our knowledge, were not used for mass surveillance in Europe. Even when data was collected on a central server, we found no reporting of data being (mis)used by governments to harass opponents and critics. This is not to say, however, that the introduction of the COVID-19 contact tracing apps did not create interferences with fundamental rights. Governments should learn lessons from the mistakes made with tracing apps to avoid the repeat of fundamental rights problems.

In our research, we have identified three main problems with the way Member State governments introduced contact tracing apps.

First, in many European countries there was no public debate on whether such apps were needed as a means to protect public health. While governments may take swift action to deal with a public health emergency, there would have been time and opportunities for a public debate. This lack of public discussion may well undermine trust in the apps as well as other measures to protect public health. Trust, in turn, is a necessary precondition

[1] https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

for widespread compliance. In the case of the tracing apps, low trust means low uptake, and, consequently, low efficiency.

Second, it seems that many governments have consulted neither authorities nor independent experts on the expected efficacy of such apps, on the social impacts of their widespread use, and on the ways potential harmful effects can be mitigated. While this may have been justified in an emergency situation, and/or in relation to the relatively few apps that were launched in the spring of 2020, it is hardly acceptable that governments kept introducing/ running apps later on without investigating their costs and benefits.

Third, governments were not transparent on what exactly they are doing with the apps and why. While a number of countries eventually published the source codes of their apps and made a data protection impact assessment available, many of them did so only months after launching the apps, and some never did. In addition, a number of governments silently abandoned the project by the second half of 2021, never allowing the interested public to investigate what exactly was happening, and what went wrong.

One year under COVID-19 contact-tracing apps: where are we?

A. The age of techno-solutionism

A year into the use of COVID-19 contact tracing apps, most European countries have developed and launched their tools, but it is unclear how efficient these tools were in limiting the spread of the virus.

Countries introduced apps in a rush, hoping that they would do something above and beyond what human contact tracers can do -- e.g., detect the potential spread between strangers on public transportation, and thereby break the chain of infections. There is no doubt that contact tracing is a needed practice to fight against a pandemic, yet this was a case of techno-solutionism: blind trust in the ability of technology to solve the problem without proper evidence of efficacy. The apps were launched before the public and experts could discuss if and how these tools could help, how they would work across the EU or not, and how these systems would impact human rights. This lack of public debate later, when the apps did not indeed break the chain of infection, potentially further decreased the trust in our democratic institutions and in science in general.

As a result of the rush, a patchwork of apps was launched, using different models that were not always compatible and thus created issues for cross-border contact tracing. Governments have also not provided much information on the use of these apps. One year later, we do not have updated or comprehensive numbers on the uptake and efficiency of these tools for each country in the EU.

B. The dependence on Big Tech

In deciding to build apps for contact tracing so quickly, governments directly or indirectly handed powers to privately owned companies that only democratically elected representatives of the people should have. The infrastructure used by most COVID-19 contact tracing apps in the EU relies on two Big Tech companies: Google and Apple. Most countries relied on solutions provided by these companies to develop their apps. These companies came up with a tech solution quickly and they decided to include some privacy standards in their models. Yet, it is deeply concerning that most governments had little-to-no choice but to use what Google and Apple offered.

At the end of the day, these two companies, not governments, decided which apps were available to all iPhone and Android users. When governments decided to conduct online contact tracing via an app, they had no genuine choice but to work with these companies in one way or another and it reaffirm these companies' powers. In addition, it is important to note that while Google and Apple made important promises regarding the use of safeguards to prevent disproportionate tracking or re-use of information in the apps, it is nearly impossible to verify these commitments as they do not allow for a full audit of their systems.[2] The COVID-19 crisis has certainly shed light on the far-reaching power of a few large companies, not just over people, but also over governments.[3]

C. Interoperability: insufficient information

As EU countries rushed to launch their contact tracing apps, they did not consult each other to ensure that the systems developed would be interoperable. As a result, many very different and incompatible apps were launched across the EU, making it difficult to track cases across borders. Interoperability, at least in the beginning, was not governments' primary goal.

The European Commission realised relatively early that the national apps need to become interoperable so that free movement, one of the basic rights of EU citizens, becomes (as) safe (as possible). The Commission launched a project to provide guidance to EU states on ensuring that measures implemented in relation to the fight against COVID-19 also guarantee the privacy of patients and users.

In April 2020, the eHealth Network adopted a common EU toolbox on COVID-19 contact tracing apps, establishing a pan-European approach.[4] Soon after, the Commission issued a Communication on Guidance on Apps supporting the fight against the COVID-19 pandemic in relation to data protection.[5] In June 2020, Member States agreed on the technical specifications of interoperability to securely exchange information between national apps based on a decentralized architecture.[6]

[2] See e.g, here, here and here.

[3] https://www.cs.ru.nl/J.H.Hoepman/publications/gaen-critique.pdf

[4] eHealth Network Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States, 15 April, 2020

[5] COMMUNICATION FROM THE COMMISSION Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, Brussels, 16.4.2020 C(2020) 2523 final https://ec.europa.eu/info/sites/default/files/5_en_act_part1_v3.pdf

[6] Interoperability guidelines for approved contact tracing mobile applications in the EU, 13 May, 2020.

Finally, in autumn 2020, the Commission launched the EU interoperability gateway. Through this service, EU countries using similar standards could add their app to the gateway to make them interoperable and function across borders. A year later, it seems that 17 apps are participating in this system. A total of 21 apps could be part of this interoperable system.[7] Based on the Commission's information, we also understand that countries like France or Hungary who have centralised apps may not be able to participate in this programme as the technical characteristics of these apps are a barrier to interoperability.

In late 2020, Access Now and the Civil Liberties Union for Europe sent a letter to the Commission asking for additional information on this programme including on the participating countries, the information used by the central system linking all apps and the data protection measures in place. Five months later, we received a response from the Commission, inviting us to consult their dedicated website to learn about the project. This response did not answer our specific questions on the functioning of the system. The information publicly available on the site is not sufficient to understand how the interoperability gateway is functioning and what has been done by the Commission to ensure General Data Protection Regulation (GDPR) compliant solutions.

What is more, in our letter, we pointed out unresolved data protection issues with the deployment of national COVID-19 apps. Based on our research,[8] we know that in some countries, data protection impact assessments were not conducted or only in a limited manner and had to be repeated after the launch of the app, or data controllers did not consult the data protection authorities before launching the app, such as in Czechia, Poland, Hungary, Slovenia and Spain.[9] This is not in line with obligations set by the GDPR. The European Commission has prepared a document providing information on the European Federation of the Gateway System (EFGS) that can be used by the Member States as a component of their respective data protection impact assessments for the exchange of personal data via the Gateway. In its response to our letter pointing to issues with the lack of impact assessments, the Commission indicated that "the enforcement of data protection rules in the EU is the responsibility of the Member States' data protection authorities. The Commission as the Guardian of the Treaties monitors that Member States comply with EU law." We do not dispute these facts. On the contrary, this is exactly why the Commission should ask the concerned Member States why they have failed to conduct such impact assessments.

[7] https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic-old/mobile-contact-tracing-apps-eu-member-states_en

[8] COVID-19 Technology in the EU: A Bittersweet Victory for Human Rights?, Civil Liberties Union for Europe, 2021.

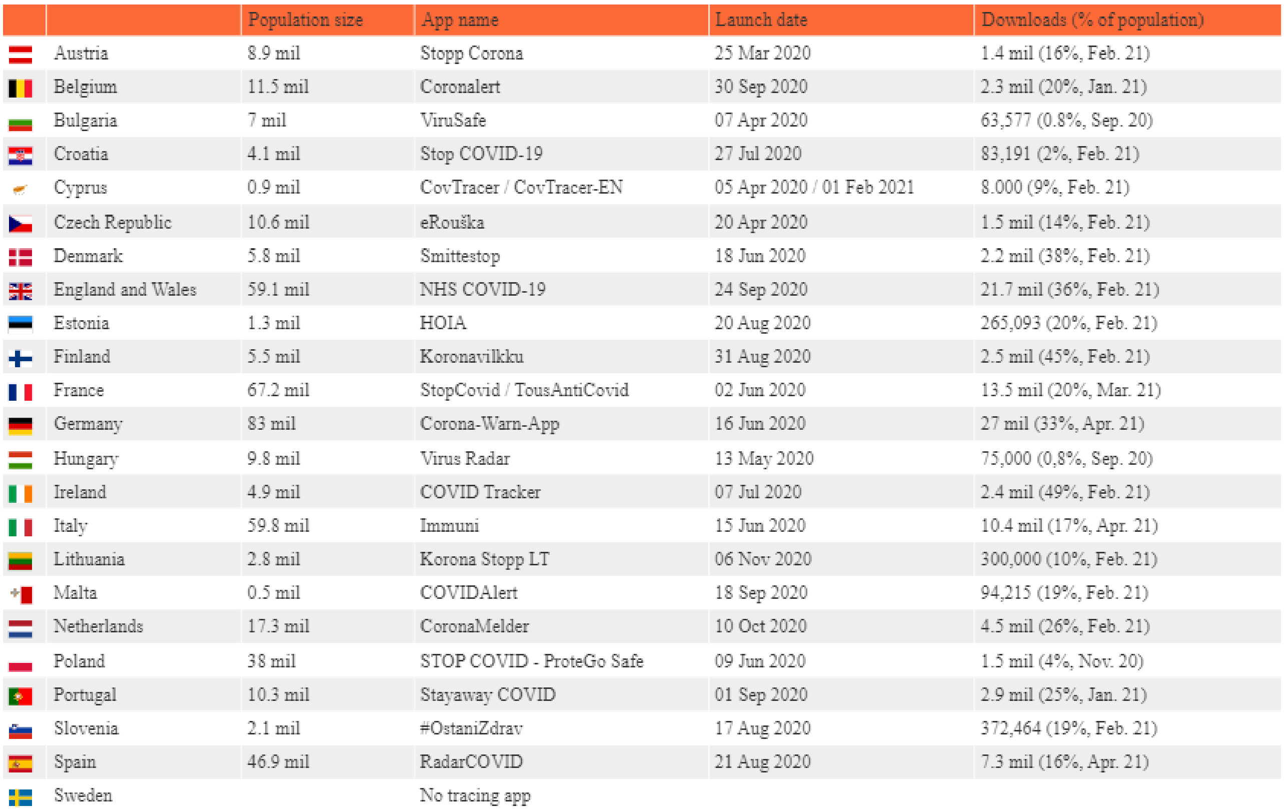
[9] https://dq4n3btxmr8c9.cloudfront.net/files/c-5f-T/Liberties_Research_EU_Covid19_Tracing_Apps.pdf

D. Communication and trust: why don't people trust governments?

According to our research, the use of the COVID-19 tracing applications was limited. In early 2021, the download rate of the application was comparatively high in Ireland (49%), Finland (45%), Denmark (38%), and Germany (30%). These countries made all relevant information about the apps publicly available, governments conducted public debates, and they made sure that their app's source code is in the public domain. However, in most of the EU countries, the download rate was less than 20% and governments did not make all relevant information readily available.

In researching what could explain the low uptake of contact tracing apps, we considered the issue of lack of public trust. Broadly speaking, trust in institutions is based on two factors. First, whether the public thinks the institution is taking the right course of action. Second, whether the institution can carry out that action competently to produce the desired result. Because many governments effectively imposed a technological solution that most people don't understand, without providing adequate information or hosting a public debate, and also without proof of efficacy, it's likely that this had a negative impact on public trust.

Decrease in public trust is, of course, a systematic problem and has not started with the



		Population size	App name	Launch date	Downloads (% of population)
	Austria	8.9 mil	Stopp Corona	25 Mar 2020	1.4 mil (16%, Feb. 21)
	Belgium	11.5 mil	Coronalert	30 Sep 2020	2.3 mil (20%, Jan. 21)
	Bulgaria	7 mil	ViruSafe	07 Apr 2020	63,577 (0.8%, Sep. 20)
	Croatia	4.1 mil	Stop COVID-19	27 Jul 2020	83,191 (2%, Feb. 21)
	Cyprus	0.9 mil	CovTracer / CovTracer-EN	05 Apr 2020 / 01 Feb 2021	8.000 (9%, Feb. 21)
	Czech Republic	10.6 mil	eRouška	20 Apr 2020	1.5 mil (14%, Feb. 21)
	Denmark	5.8 mil	Smittestop	18 Jun 2020	2.2 mil (38%, Feb. 21)
	England and Wales	59.1 mil	NHS COVID-19	24 Sep 2020	21.7 mil (36%, Feb. 21)
	Estonia	1.3 mil	HOIA	20 Aug 2020	265,093 (20%, Feb. 21)
	Finland	5.5 mil	Koronavilkku	31 Aug 2020	2.5 mil (45%, Feb. 21)
	France	67.2 mil	StopCovid / TousAntiCovid	02 Jun 2020	13.5 mil (20%, Mar. 21)
	Germany	83 mil	Corona-Warn-App	16 Jun 2020	27 mil (33%, Apr. 21)
	Hungary	9.8 mil	Virus Radar	13 May 2020	75,000 (0,8%, Sep. 20)
	Ireland	4.9 mil	COVID Tracker	07 Jul 2020	2.4 mil (49%, Feb. 21)
	Italy	59.8 mil	Immuni	15 Jun 2020	10.4 mil (17%, Apr. 21)
	Lithuania	2.8 mil	Korona Stopp LT	06 Nov 2020	300,000 (10%, Feb. 21)
	Malta	0.5 mil	COVIDAlert	18 Sep 2020	94,215 (19%, Feb. 21)
	Netherlands	17.3 mil	CoronaMelder	10 Oct 2020	4.5 mil (26%, Feb. 21)
	Poland	38 mil	STOP COVID - ProteGo Safe	09 Jun 2020	1.5 mil (4%, Nov. 20)
	Portugal	10.3 mil	Stayaway COVID	01 Sep 2020	2.9 mil (25%, Jan. 21)
	Slovenia	2.1 mil	#OstaniZdrav	17 Aug 2020	372,464 (19%, Feb. 21)
	Spain	46.9 mil	RadarCOVID	21 Aug 2020	7.3 mil (16%, Apr. 21)
	Sweden		No tracing app		

Source: Civil Liberties Union for Europe pandemic. However, there is no doubt that as the pandemic hit the world, uncertainty increased to a level that also further impacted the trust in democratic institutions. Governments and authorities, such as the World Health Organization, communicated confusing messages about the virus, its impact, and how to tackle the problem, for example, on whether it makes sense for civilians to use masks. The Chinese censorship[10] around the virus started in November 2019 even amplified the uncertainty and the mistrust in governments and in the mainstream media.

Social mistrust varies according to social status, digital skills, and access to technology. The digital divide pushes the vulnerable groups to feel they benefit less, especially in relation to access to health care and to the vaccines' impacts. The social divide transformed to a digital divide that has further transformed to a data divide: the access to data-driven technologies such as the digital health technologies.

European governments have a lot to do. First and foremost, the aim should be to regain and rebuild trust in democratic institutions that would also help in any emergency situation in the future.

Transparency and accountability of governments are key. Responding to freedom of information requests in time and in a meaningful way would help communication between governments and journalists and civilians. To mention our own experience with the Commission: it took almost five months to get a response to our letter, and we did not get answers to our concrete questions regarding the interoperability of tracing applications. In some EU countries during the first year of the pandemic, press conferences were suspended, and journalists could not ask questions, not even related to the pandemic. In a few Member States, such as Italy, Hungary, and Slovenia, the deadline for answering freedom of information requests was significantly extended.[11]

[10] Reporters Without Borders, 6 May, 2020.

[11] IFEX, 6 June, 2020.

Conclusion

Member States' solutions to mitigate the effects of the pandemic were to a significant extent technology-driven. Vaccine research, tracing and quarantine applications, and the new normal for working and studying from home are all connected to technological solutions. Some of these improved our lives enormously, while others failed to do so. Those that were perceived to be failing may, in the long-term, have a negative impact on public trust.

We fully agree with the Ada Lovelace Institute that the "effective deployment of technology to support the transition from the crisis will be contingent on public trust and confidence".[12] After many scandals, including Cambridge Analytica, people are increasingly aware of the potential risks linked with governments, authorities, and political actors using their data. Public trust must be restored both towards certain technologies and towards governments, authorities, and societies as a whole. One of the lessons that must be learned of the pandemic is that governments must act responsibly and transparently when it comes to offering solutions for social problems with technology.

Personal data protection and the enforcement of the General Data Protection Regulation is an essential part of this process. If governments can be held accountable for their actions, if data collection is transparent, and the outcomes of research and data analysis are communicated directly and clearly, that helps restore social trust. Restoring social trust would impact the relationship between governments and citizens and abiding rules, using technology, and solidarity.

By now, we understand that the rushed deployment of technical solutions is at a deadlock. Supporting evidence for an effective technological solution, publicly available data, transparent communication, and accountable governments are key to regaining social trust. Technology will never be the answer to social crises but only a tool, whether that be an emergency like the COVID-19 pandemic or other catastrophes. But proper technical solutions, privacy by design, and digital inclusion could support measures to mitigate emergency situations.

Recommendations for the future - building more trust

1. **Governments' contracts and purchase of technology should be transparent.**

The experience with the contact tracing apps shows that in countries where the government communicated openly and clearly on what kind of app they would like to get developed or purchased and why, where they published

[12] https://www.adalovelaceinstitute.org/news/exit-through-the-app-store-uk-technology-transition-covid-19-crisis/

documentation connected to the app (e.g, data protection impact assessment, source code), people were more willing to download the app and, presumably, to comply with its recommendations. Governments must act transparently when it comes to offering solutions for social problems with technology.

2. Governments' dependence on Big Tech should be addressed by promoting competition, stronger oversight, and decentralised infrastructure.

The experience with the contact tracing apps confirms that governments are dependent on a few private actors, especially when they try to solve crises. We need strong oversight of Big Tech to ensure proper transparency of algorithms, promote privacy by design, and human rights impact assessment. The enforcement of existing and future competition rules must be supported with further safeguards to fundamental rights.

3. Governments should avoid overselling new technological solutions.

The experience with the contact tracing apps shows that overselling new technology diminishes trust in a system that will not function efficiently without public trust.

4. The EU and Member States should communicate in a clear and timely manner with the public and rights groups.

While the pandemic may have justified some initial slowness in response, at least in topics not connected to the ongoing crisis, citizens have a focal interest in being able to learn how exactly the crisis is handled and what measures are taken and for what reason. Thus, press briefings and responding to freedom of information requests in a timely and meaningful way are crucial both for regaining social trust and effectively containing emergency situations.

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting and protecting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of national civil liberties NGOs from across the EU. Unless otherwise indicated, the opinions expressed by Liberties do not necessarily constitute the views of our member organisations.

Website:

liberties.eu

Contact info:

info@liberties.eu

The Civil Liberties Union for Europe e. V.

Ringbahnstr. 16-20
12099 Berlin
Germany

Subscribe to our newsletter

https://www.liberties.eu/en/subscribe

Reference link to study

Please, when referring to this study, use the following web address:
https://www.liberties.eu/f/xs_La1

Follow us

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

accessnow.org