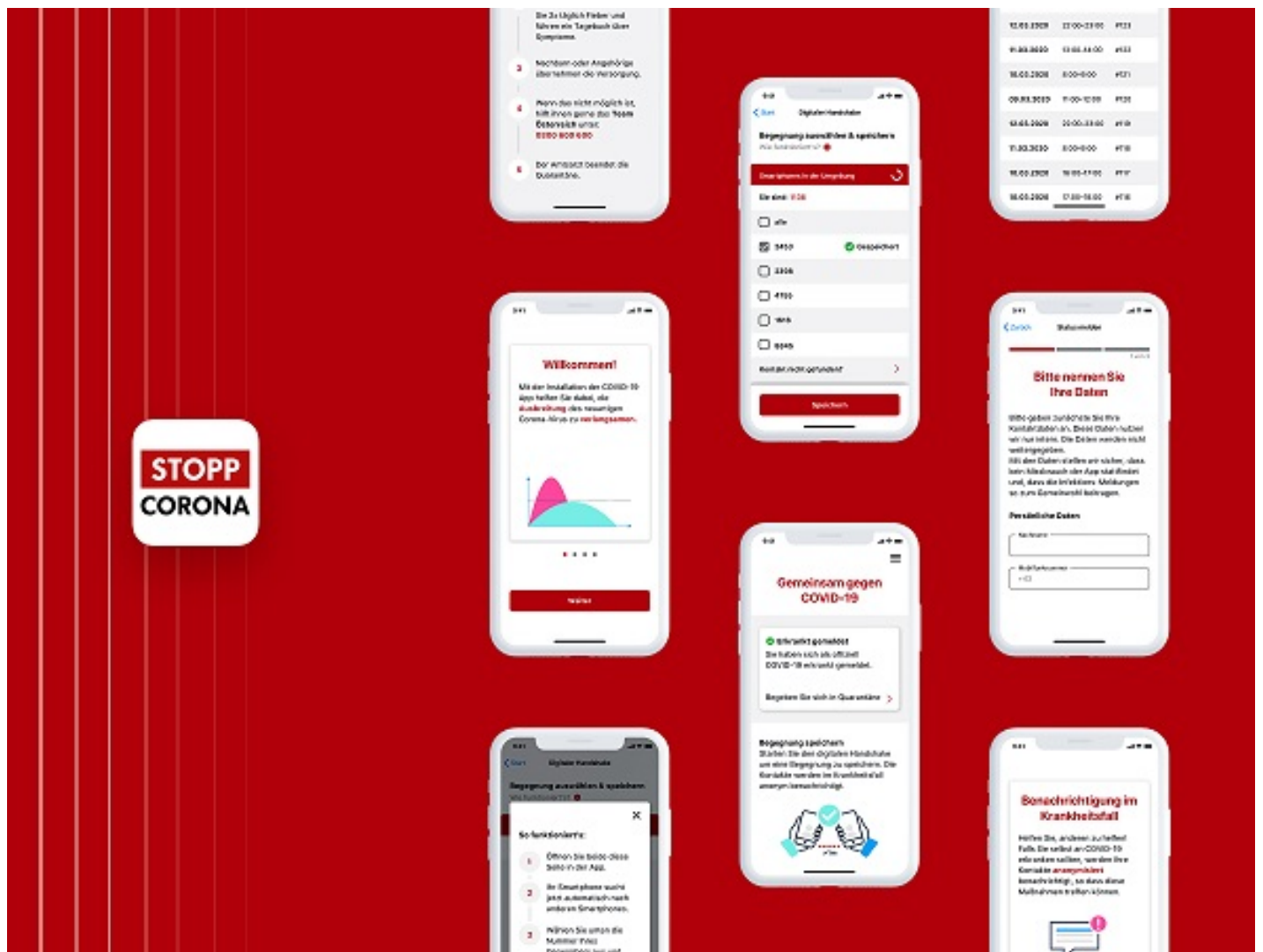


# COVID-19 and contact tracing: a call for digital diligence

May 13, 2020, Analysis / COVID-19 and conflict / Humanitarian Action / New Technologies

Balthasar Staehelin & Cécile Aptel



As the COVID-19 pandemic continues to impact society worldwide, contact tracing apps are being developed in a bid to contain the spread of the virus. The Red Cross and Red Crescent Movement, a global humanitarian network with a long experience of working on health issues, including in the most challenging contexts, is inherently concerned with the debate on contact tracing.

*In this blog, Balthasar Staehelin, ICRC's Director of Digital Transformation and Data, and Cecile Aptel, Director of Policy, Strategy and Knowledge for the International Federation of Red Cross and Red Crescent Societies, offer a perspective on why and how the humanitarian principle of 'do no harm' must extend today to 'do no digital harm', safeguarding the principle of humanity at the core of any policy. How can digital contact tracing be most appropriately used to save lives while respecting individual rights, including the right to privacy?*

00:00

00:00

Contact tracing is an established means to *fight the spread of infection* in populations when integrated within a broader and holistic health response strategy. Traditionally a manual process of identifying who an infected person may have come into contact with while they were contagious, it is time consuming and challenging to scale up to cover larger populations. To accelerate and scale the response to the current COVID-19 pandemic, new technology solutions are being designed and developed.

The use of mobile phones for '*contact tracing*' apps has gained significant traction in the last few weeks. This has led to a dynamic and intense debate at the crossroads of public health, data protection and privacy. Trust in technology, and potential economic and strategic interests are also central to the discussion. We are concerned that unsuitable design or usage of such apps could lead to stigmatization, increased vulnerability and fragility, discrimination, persecution, and attacks on the physical and psychological integrity of certain populations. This touches upon the larger question of the responsible use of technology in contexts such as crisis response, wherein trust is central<sup>[1]</sup>.

## **Contact tracing: what are the potential risks?**

In many places where the Red Cross Red Crescent Movement works, people often share one smartphone with other family members. They can leave their phone at charging stations hosting dozens of other devices. Similarly, people can be in the same space but protected by masks or separated by a window or plexiglass. Thus, in different contexts, complex human interactions and social habits, or relatively low digital literacy levels, may render the use of precise apps or the key technologies (such as Bluetooth) ineffective.

In contexts where access to smartphones and internet may not be sufficient to provide the minimum effective uptake, a technology that relies on proximity sensors of mobile phones could be severely impaired. Even with an overall high usage of modern smartphones, the risk of excluding or marginalizing the less connected parts of the population exists, leaving the most vulnerable behind, and ultimately eroding the utility of contact tracing.

The risk that data collected for the purpose of contact tracing may be used for other purposes – or connected with other data sets to identify and potentially further profile individuals – is a central concern. This ‘scope creep’ could lead to intrusive surveillance or unsolicited and undesirable commercial use. In contexts affected by armed conflict, violence or disaster, such practices can have severe humanitarian consequences. Any, or a combination of these, could significantly erode the trust that people have in contact tracing, in the public health response and in those that promote it. Without that trust, the uptake and the desired effectiveness of such applications would be reduced.

In parallel, contact tracing apps are not immune to cyber attacks and data leakages which could expose the privacy and security of their users. The consequences of the exposure of private and personal data in a polarized environment, based on ethnic or communal tensions or on economic inequalities, would be of great concern.

## **What does successful contact tracing look like?**

For digital contact tracing to be a successful component of the response to a pandemic, a strong public health system should be in place to shoulder the necessary follow-up actions, such as offering adequate testing, isolation and treatment facilities. This underlines again the need for long-term sustained investment in health systems.

Digital contact tracing also needs solid and effective checks and balances to control its effectiveness and ensure a transparent and fair management of the overall ecosystem; public health and individual rights, especially in relation to privacy, must be able to work hand in hand. This is not possible in every country, and even more challenging in fragile environments affected by armed conflict, violence or disaster where the power to act and the resources of the State have often been severely undermined.

An evaluation of these turnkey elements requires a case by case assessment, with an in-depth knowledge of context. It is impossible to determine in absolute terms all aspects – or the potential and pitfalls – of the digital contact tracing apps that are currently being considered or deployed in many parts of the world. However, based on our humanitarian experience and specific expertise in data protection, the benefits and risks of contract tracing must be meticulously weighed up. Up-to-date scientific, ethical and legal standards should be firmly built into this process, and only solutions that are based on a ‘data protection by design’ approach should be considered valid.

Applying ‘data protection by design’ is central to ensuring the respect of the humanitarian ‘do no harm’ principle and the rights and dignity of the individuals concerned. In this context, ‘data protection by design’ hinges on a decentralized architecture designed to keep as much sensitive data as possible on users’ devices. Other essential characteristics include purpose limitation to mitigate ‘scope creep’, and a fixed data retention period, ensuring that digital contact tracing tools are promptly decommissioned once they are no longer necessary. A number of digital contact tracing protocols designed to help contain the spread of COVID-19 have been developed and already reviewed considering data protection in humanitarian action. One notable example of such a decentralized protocol, proposed by the *DP-3T consortium* and subsequently adopted by the *Austrian Red Cross* and supported by the *Apple/Google initiative*, is gaining significant traction.

## Conclusion: a call for digital diligence

Over its long history, the Movement has amassed a vast collective experience of both the opportunities and risks that new technology can unleash into humanitarian settings. Now, in the face of a pandemic threatening millions around the world, we are again witnessing the draw of its advantages, as well as the concerns surrounding its risks. Contact tracing apps offer very real potential to curb the spread of the virus; but they bring up considerable data privacy and other concerns.

In this light, States should assess whether a mobile-based contact tracing app could be an appropriate, effective, ethical and safe component of the COVID-19 response in their particular context to save lives. If a State determines that it would be, it should undertake a careful balancing of the benefits and risks to use a decentralized protocol such as DP-3T, and to incorporate 'data protection by design' and up-to-date scientific, ethical and legal standards in its responses.

[1] An issue that gave raise to substantial discussions at the recent *33rd International Conference of the Red Cross and Red Crescent Movement*.

### See also

- Cordula Droege, *COVID-19 response in conflict zones hinges on respect for international humanitarian law*, April 16, 2020
- Massimo Marelli, *Hacking Humanitarians: moving towards a humanitarian cybersecurity strategy*, January 16, 2020
- Delphine van Solinge, *Digital risks for populations in armed conflict: Five key gaps the humanitarian sector should address*, June 12, 2019

Tags: *Austrian Red Cross, contact tracing, Coronavirus, COVID-19, data protection, do no harm, humanitarian principles, pandemic*

---

Share this article   

---

## Comments

MUNEER TAHER, 13 May 2020

Assist to fight Covid-19, well done

---