Cyber Pandemics

Barbara Carminati, *University of Insubria, 21100, Varese, Italy*
Leila Bahri, *KTH Royal Institute of Technology, 114 28, Stockholm, Sweden*

The focus of this special issue is on studying the consequences of pandemics and cyber pandemics on privacy and trust both in the digital and the real worlds. In the aftermath of the recent COVID-19 pandemic that has shaken several aspects of our lives for almost two years of time, preliminary research indicates that the technological capabilities and the data that have been deployed and exploited to contain the spread of the disease may have affected people's privacy, sense of security, as well as their trust in their governing institutions. The enclosed articles explore both the effectiveness and the impacts of some of the deployed technologies in the handling of the COVID-19 pandemic on people's privacy as well as on their security and related risks.

In recent years, the main way to stop serious epidemics and pandemics, such as the plague and cholera, has been to limit contact between people, especially between sick and healthy people. This action was taken in an effort to contain the spread of the disease. The same public health strategy has been widely employed to prevent the spread of COVID-19 and maintain social cohesion. However, in contrast to the past, during the COVID-19 pandemic, we were able to exploit advanced technological capabilities. In addition to social distance, the data-driven society we live in has enabled governments to track and contain the spread of COVID-19 more effectively, leveraging data analytics to analyze trends, detect cases faster, and provide targeted responses.

While these have definitely helped in handling the emergency and reducing the spread of COVID-19, preliminary research indicates that they may have had a significant impact on people's perceptions of their own privacy as well as their trust in technologies and systems. For example, there has been a lot of discussion about the effects of more surveillance systems and the use of facial recognition to enforce quarantine rules.

At the same time, social distancing and lockdowns have shifted almost all aspects of human communication, including those related to work activities, to the digital space. This significant increase in reliance on digital communications, as well as the sudden need for its adoption in various contexts, has created an opportunity for cybersecurity criminals and opportunists. With more and more assets online, cyberattacks become more profitable and offer a better return on investment. An increase in cyberattacks, which have the potential to be pandemic in terms of spread and impacts on society, is a risk that cannot be ignored.

The goal of this special issue is to investigate the consequences of pandemics on individual privacy and trust in governments and technologies, as well as to examine how the privacy and trust landscapes have evolved, including the related security and privacy risks.

The first paper, "When Privacy, Distrust, and Misinformation Cause Worry About Using COVID-19 Contact-Tracing Apps," reviews the available literature on contact tracing apps that have been deployed by some governments to contain the spread of the COVID-19 disease in order to study their effective adoption in the populations as well as the impacts they had on people's privacy by scrutinizing the types and amounts of personal data involved and how it is processed. Although such contact tracing apps could be critical in the containment of the spread of such diseases, their power remains in the level of their acceptance by the people. For this, the paper synthesizes on possible techniques that could help the promotion of such contact tracing apps and increase their acceptance and adoption by the people in a privacy preserving manner.

The second paper, "Privacy and Integrity Threats in Contact Tracing Systems and Their Mitigations" also approaches contact tracing apps but this time with a focus on security, possible attacks, and their effects

1089-7801 © 2023 IEEE
Digital Object Identifier 10.1109/MIC.2023.3237239
Date of current version 14 March 2023.

on privacy and trust. The paper does so by analyzing the decentralized contact tracing solution known as Google and Apple Exposure Notification system. The paper studies the vulnerability of the system to a number of known and new security attacks and exposes some privacy and integrity issues. The paper also presents solutions to secure against these attacks and proposes an alternative with more resilience to the identified attacks.

Truth of the matter is that new technologies and the data connected world we live in nowadays should enable and simplify the containment of pandemics. However, the usage of technologies, such as contact tracing apps, could be intrusive to people's rights and freedoms. This can affect people's trust in such systems and limit their adoption, which in turn would inhibit their effectiveness in achieving the purpose of disease containment.

BARBARA CARMINATI is with the University of Insubria, 21100, Varese, Italy. Contact her at barbara.carminati@uninsubria.it.

LEILA BAHRI is with the KTH Royal Institute of Technology, 114 28, Stockholm, Sweden. Contact her at lbahri@kth.se.