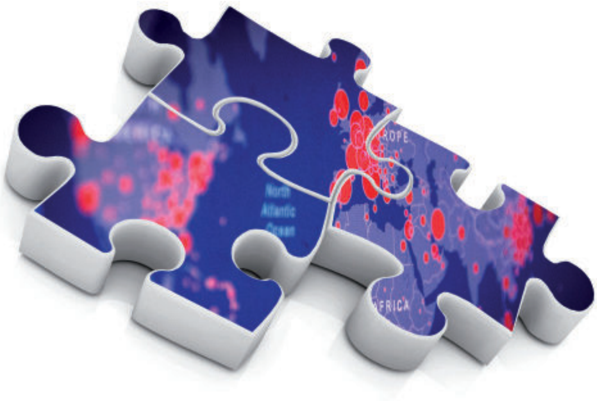

Technology in Conflict:

How COVID-19 Contact Tracing Apps can Exacerbate Violent Conflicts

Jennifer Easterday

STRATEGIC UPDATE
AUGUST 2020

LSE IDEAS is LSE's foreign policy think tank. Ranked #1 university affiliated think tank in the world in the 2019 Global Go To Think Tank Index.

We connect academic knowledge of diplomacy and strategy with the people who use it.

> “
>
> Advances in AI technology are being exploited as tactics in asymmetric warfare, and facial recognition is being used to repress and surveil on a mass scale. Contact tracing tools developed to stop the spread of COVID-19 are no exception—they pose significant risks to human security.

By now, it is widely accepted by companies and civil society alike that the promise of technology to support human rights and human security has a dark inverse—it has become a powerful weapon for fomenting violence, conflict, and abuse. Social media has been used to further large-scale human rights abuses, armed conflict, and mass killings in places like Myanmar,[1] India,[2] Sri Lanka,[3] and elsewhere.[4] It is used to coordinate and direct[5] hate-based violence in the United States[6] and was used to promote a terrorist attack in New Zealand.[7] Advances in AI technology are being exploited as tactics in asymmetric warfare,[8] and facial recognition is being used to repress and surveil[9] on a mass scale.[10] And contact tracing tools developed to stop the spread of COVID-19 are no exception—they pose significant risks to human security.[11]

Emerging research shows that these risks are much more acute in markets that have a history of conflict or mass human rights abuses. In those contexts, the scope and scale of potential harms are significant. This is true whether we are evaluating the impact of hate speech and misinformation or the use of facial recognition for mass surveillance. It is also true when we look at the potential negative impacts of COVID-19 tech tools.

COVID-19 and contact tracing pose risks for human security

With the outbreak of the COVID-19 global pandemic, governments all over the world ordered people to stay at home and started to look for ways to stop the virus from spreading. One established method for stemming viral infections is contact tracing—investigating all contacts made by a person who is infected by the virus. It is traditionally done manually, and can be time consuming. To scale up the ability to use contact tracing to track and fight COVID-19 outbreaks, governments and private companies partnered to develop new technology tools.

Some of these, called contact tracing apps,[12] use location tracking or proximity[13] tracking[14] to identify when a user has been near someone who has been diagnosed with COVID-19. Some[15] of them[16] even track users' locations. This is used to understand where outbreaks start and how they spread, and can be used to quarantine those who have come into contact with infected people. Other governments are partnering with private companies to create websites for users to input health and personal data for COVID-19 screening, or to create data management systems[17] to help with manual contact tracing efforts.

> China built a mandatory smartphone app to track the movements of huge numbers of people in the wake of the COVID-19 outbreak. It can impose restrictions on movement, and appears to send personal data to police. This is especially risky in a country that has used facial recognition surveillance to target ethnic minorities.

There are many examples where countries have implemented these tools without proper privacy protections and where they pose a risk for human security. China built a mandatory smartphone app to track the movements[18] of huge numbers of people in the wake of the COVID-19 outbreak. It can impose restrictions on movement, and appears to send personal data to police. This is especially risky in a country that has used facial recognition surveillance to target ethnic minorities.[19] In Guatemala,[20] a contact tracing app collects data about users' exact location, even when the app is closed. The data can be held for up to ten years, and the President has indicated that he hopes the app will evolve to cover "security issues." In Israel, the government has turned to cell phone location data to conduct contact tracing and order individualized quarantines[21]. NSO, an Israeli company infamous for the Pegasus spyware software that it develops, had developed a contact tracing tool that analyzes huge volumes of data to map people's movements and contacts.[22] Nearly a dozen countries are reportedly testing[23] this tool. This is part of a wave of surveillance companies repurposing spy and law enforcement tools[24] to track the coronavirus and enforce quarantines. In Ethiopia,[25] the state released a COVID-19 monitoring platform[26] where users can report others suspected of having symptoms—based on subjective assessments of their symptoms. This is particularly concerning in that context, given the reports of harassment and discrimination against foreigners[27] and healthcare workers[28]. And there are many, many other problematic examples.[29]

Of course, in the face of a global pandemic, there are legitimate tradeoffs that governments can make. Some privacy violations might be necessary, as long as they are proportionate and strictly limited to COVID-19 efforts. Moreover, there are positive applications of technology which can deliver effective responses to COVID-19, not only in mitigating the health consequences of the pandemic, but also in protecting livelihoods and generating alternative economic opportunities despite the virus.

The effectiveness of these tools is still uncertain, especially for communities where smartphone penetration is low. Many of the tools fail to take into account systemic inequalities in how people access the internet. Technology use also discounts living conditions for many of the world's most vulnerable populations, where users are not necessarily individually linked to a mobile phone. For example, migrant workers in the Persian Gulf often share a phone; refugees living in camps are known to switch between multiple SIM cards; and people often share one smartphone with other family members.

What is certain, however, is that in high-vulnerability contexts, these COVID-19 tech tools pose a number of serious risks to human security, yet also have the potential to enhance human security in the face of the threat of health, social and economic disruption..

The challenge, therefore, is to put in place guidance and methodologies that guard against mis- or unintended use of technology while also directing effectively its positive potential. A human security approach to technology seeks to broaden the horizon of potential harms by considering the comprehensive and interrelated nature of threats to people from the increased use of technology. At the same time, human security methodology is also about empowering people in spite of their vulnerability and apparent powerlessness. In this sense, a human security approach to tech responses to COVID-19 considers how tech companies, governments, and other actors can intervene to work with communities in ways that enhance their agency in the face of the pandemic.

> “The COVID-19 contact tracing tech tools fits within a larger problem with the weaponization of technology and lack of regulation more generally.”

Civil society responses to mitigate harm

The International Committee of the Red Cross (ICRC) warns[30] that the “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.” It calls for technology companies developing these apps to employ “data protection by design” and other responsible technology practices. The ICRC notes that misuse of contact tracing technology can impair trust in public health responses to the outbreak and further exacerbate outbreaks in those communities.

Amnesty International[31] also calls for companies and governments designing contact tracing apps to build in privacy and data protection by design, among other recommendations.[32] This means that any data collected must be the minimum amount necessary, must be securely stored, and must be collected strictly for the purpose of controlling the spread of COVID-19. Data should be anonymized, even when combined with other data sets. It should not be used for law enforcement, national security, or immigration purposes, nor should it be made available for commercial use.

Human Rights Watch[33] warns that using contact tracing apps will disproportionately impact already-vulnerable populations.[34] There is the risk that governments will collect more data than is strictly necessary to track and treat COVID-19 outbreaks—and that it will continue after the pandemic is contained. Many lack transparency or legislative oversight and limitations. Many of the governments using technology to collect data about COVID-19 have a history of pervasive surveillance and repression and discrimination against marginalized communities.

Privacy International directly warns that[35] “we must build crisis-era tech with the presumption that it will be used in a country with weak rights protections, and that it will ultimately be used against the people it’s designed to protect.”

Interrelated and comprehensive impacts

While the privacy and human rights risks are significant, what is more concerning is the potential for these tech tools to cause or intensify violent conflict. Many of the governments using some of the most privacy-violating versions of contact tracing and other COVID-19 tech tools have histories of conflict and mass human rights abuses. These tools can easily be weaponized to further repression, surveillance, discrimination, and violence in those areas. Where government intentions are good, poorly designed and implemented COVID-19 tech tools can nonetheless undermine fragile trust in governments and public health authorities. It can impair legitimacy of state actors in situations where this can entrench perceptions of injustice and abuse—often root causes of conflict.

Many communities experienced an uptick in violence[36] due to COVID-19 policy responses and flaring tensions exacerbated by increases in food insecurity, job losses, and other grievances. The pandemic, and responses to it, disproportionately impact[37] communities that have long-suffered from socio-economic hardships, human rights abuses, exclusion, and discrimination.

The COVID-19 contact tracing tech tools fits within a larger problem with the weaponization of technology and lack of regulation more generally. Much has been said about the potential impact of technology on human rights, in particular the right to privacy and freedom of expression. But we need to evolve that conversation and take a systemic look at how technology and human rights abuses contribute to violence and conflict in high-risk markets.

There are many ways that tech companies are inadvertently contributing to conflict dynamics through product design and release decisions. Sometimes technology products are used by third parties in order to foment conflict and abuse. Content moderation on social media platforms can also exacerbate a conflict. So can following government orders to shutdown internet services, or collect and process sensitive data. Sometimes just releasing a product or service in a conflict-affected market can have adverse impacts on the conflict.

Ineffective and lagging policy responses

In the wake of protests against racism and police brutality in Minneapolis, Minnesota Public Safety Commissioner John Harrington compared police investigations into arrested protesters to contact tracing for COVID-19. He was referring to standard police work—which does not involve using COVID-19 contact tracing[38] or public health authorities.

It was a reckless choice of words that highlights an important example of how little the US public trusts law enforcement and potentially now, public health efforts to fight COVID-19. It also highlights a very real risk. There is no legislation in Minnesota that would prohibit law enforcement from using data collected by coronavirus contact tracers. In fact, other local governments in the United States have shared names and addresses[39] of people who have tested positive for COVID-19 with police and first responders.

This is an issue that the Electronic Frontier Foundation has raised extensively. “We need new laws to guarantee such data minimization, not just for contact tracing, but for all COVID-19 responses that gather personal information,” Adam Schwartz, senior staff attorney for the EFF, recently wrote.[40]

Technology’s role in facilitating human rights abuse and inciting violence has become an emerging concern of regulators and civil society. They have made calls for improvements to corporate regulation, both internal and external. But even as these risks are becoming apparent, there is little public accountability for the actions of tech companies large or small. The relevant domestic and international regulatory landscapes are fragmented, reactionary, and ill-equipped to respond in effective and systematic ways. Legal responses have also led to new concerns about undue restrictions on freedom of expression, a lack of due process, and abuse of regulation to create further opportunities for human rights abuse or inciting conflict. In the absence of effective state or international law, it is important to turn to industry-led regulation and multi-stakeholder initiatives that promote accountability, but also safeguard and underpin the agency of tech users.

Integrated and holistic responses

Other industries have developed multi-stakeholder processes—involving partnerships between private industry, civil society, and governments—to establish accountability norms for human rights and conflict sensitivity. Examples include the Extractive Industries Transparency Initiative,[41] the Voluntary Principles on Security and Human Rights,[42] and the Kimberley Process for the Certification of Diamonds.[43] However, there is nothing similar for the technology industry tied specifically to human security and conflict. Conflict-sensitivity and business and human rights guidance created for other industries are ill-suited for the tech industry. Most business and human rights and conflict sensitivity initiatives fail to specifically address many issues unique to rapidly changing technologies and their impact on conflict and human security. Technology companies face unique challenges and typically have business structures that require bespoke, carefully crafted policies and practices. At present, we do not know how companies perceive, react to, and operationalize these norms at scale. Nor do we have a clear understanding of how those actions translate into preventing abuse and violence on the ground or how they can be leveraged to deliver human security in the sense of protection and empowerment of individuals.

This gives rise to an urgent need to understand how these technologies—including the near ubiquitous adoption of COVID-19 contact tracing apps—impact conflict, vulnerable communities, and what good regulation looks like. ■

Notes

[1] www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

[2] www.bbc.com/news/world-asia-india-45140158

[3] www.nytimes.com/2019/04/21/world/asia/sri-lanka-social-media.html

[4] toda.org/policy-briefs-and-resources/social-media-technology-and-peacebuilding.html

[5] www.bellingcat.com/news/2020/05/27/the-boogaloo-movement-is-not-what-you-think/

[6] www.nytimes.com/2019/08/03/us/patrick-crusius-el-paso-shooter-manifesto.html

[7] edition.cnn.com/2019/03/15/tech/christchurch-internet-radicalization-intl/index.html

[8] www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/

[9] www.hrw.org/news/2019/05/31/high-tech-surveillance-china-brazil

[10] www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

[11] www.un.org/humansecurity/what-is-human-security

[12] www.eff.org/deeplinks/2020/04/covid-19-and-technology-commonly-used-terms

[13] www.eff.org/deeplinks/2020/04/apple-and-googles-covid-19-exposure-notification-api-questions-and-answers

[14] www.eff.org/deeplinks/2020/04/covid-19-and-technology-commonly-used-terms

[15] safepaths.mit.edu

[16] healthytogetherutah.com

[17] www.cnbc.com/2020/05/08/new-york-city-partners-with-salesforce-on-coronavirus-contact-tracing-program-mayor-says.html

[18] www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

[19] www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

[20] www.globalwitness.org/en/press-releases/investigation-reveals-serious-concerns-over-guatemala-covid-19-app

[21] www.washingtonpost.com/world/middle_east/israel-is-using-cellphone-surveillance-to-warn-citizens-you-may-already-be-infected/2020/03/19/68267294-69e7-11ea-b199-3a9799c54512_story.html

[22] www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus

[23] www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus

[24] www.reuters.com/article/us-health-coronavirus-spy-specialreport/special-report-cyber-intel-firms-pitch-governments-on-spy-tools-to-trace-coronavirus-idUSKCN22A2G1

[25] www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa

[26] www.covid19.et/covid-19

[27] www.france24.com/en/20200319-ethiopian-pm-urges-tolerance-as-anti-foreigner-sentiment-rises-over-virus

[28] twitter.com/ZekuZelalem/status/1247061719123472384?s=20

[29] privacyinternational.org/examples/tracking-global-response-covid-19

[30] blogs.icrc.org/law-and-policy/2020/05/13/covid-19-contact-tracing-digital-diligence/

[31] www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

[32] www.amnesty.org.uk/coronavirus/7-principles-contact-tracing-app-rollout

[33] www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa

[34] www.hrw.org/news/2020/06/04/how-digital-contact-tracing-covid-19-could-worsen-inequality

[35] privacyinternational.org/long-read/3792/covid-contact-tracing-apps-are-complicated-mess-what-you-need-know

[36] www.weforum.org/agenda/2020/04/we-need-major-cooperation-on-global-security-in-the-covid-19-era/

[37] www.ohchr.org/Documents/Issues/Migration/OHCHRGuidance_COVID19_Migrants.pdf

[38] www.vox.com/recode/2020/6/1/21277393/minnesota-protesters-contact-tracing-covid-19

[39] www.eff.org/deeplinks/2020/04/telling-police-where-people-covid-19-live-erodes-public-health

[40] www.eff.org/deeplinks/2020/06/dont-mix-policing-covid-19-contact-tracing

[41] eiti.org

[42] www.voluntaryprinciples.org

[43] www.kimberleyprocess.com/

THE AUTHOR

Jennifer Easterday is Co-Founder & Executive Director of JustPeace Labs. She is an attorney with expertise in technology and human rights law, international criminal law and peacebuilding. Her work with NGOs and international tribunals focuses on strengthening international responses to armed conflict and mass human rights abuses in Africa, Latin America and Europe.

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

EXECUTIVE MASTERS PROGRAMME

INTERNATIONAL STRATEGY AND DIPLOMACY

LSE IDEAS, a Centre for the study of international affairs, brings together academics and policy-makers to think strategically about world events.

This one year **EXECUTIVE MASTERS PROGRAMME** is at the heart of that endeavour. While studying in a world-leading university you will be able to learn from top LSE academics and senior policy practitioners.

The programme will sharpen your ability to challenge conventional thinking, explore new techniques for addressing risk and threats, and coach you in devising effective strategies to address them.

The course has been especially tailored so that you can accelerate your career while holding a demanding position in the public or private sector.

> "Right from the first week I was able to apply the lessons I had learnt to our operational and policy work and to coach my teams to look at issues differently."
>
> – **Karen Pierce**
> **British Ambassador**
> **to the United States**

CONTACT US

ideas.strategy@lse.ac.uk
+44 (0)20 7955 6526
lse.ac.uk/ideas/exec

Technology in Conflict:

How COVID-19 Contact Tracing Apps can Exacerbate Violent Conflicts

Jennifer Easterday

With the outbreak of the COVID-19 global pandemic, governments and private companies partnered to develop contact tracing apps to stem the tide of infections. But there are serious human security risks when using contact tracing apps in highly vulnerable communities. There is an urgent need for guidance and methodologies that guard against mis- or unintended use of technology while also directing effectively its positive potential. In this strategic update, Jennifer Easterday explores how a human security approach to COVID-19 tech tools would prompt tech companies, governments, and other actors to work with communities in ways that enhance their agency in the face of the pandemic to both reduce the risk of exacerbating conflict while maximizing the benefits of technology.

For general enquiries:

LSE IDEAS
Floor 9, Pankhurst House
1 Clement's Inn, London
WC2A 2AZ

☎ +44 (0)20 7955 6101

✉ ideas@lse.ac.uk

lse.ac.uk/ideas

@lseideas

lseideas

Photo credit:
Giacomo Carra
via unsplash.com