The Digital Response to the Outbreak of COVID-19

Undeniably, we need to use technology as part of disaster response, but the regulatory immaturity of the industry makes technology companies risky allies, even in the best of circumstances

Author: Sean McDonald
March 30, 2020
Art by Ben Giles

In every major disaster response, there’s a mobilization of hopeful, well-intentioned actors who try to leverage their professional skills as part of the effort — and among them, there is arguably no industry whose work is more potentially invasive or dangerous during disaster than technology. Undeniably, we need to use technology as part of disaster response, but the regulatory immaturity of the industry has made technology companies risky allies, even in the best of circumstances. And these are not the best of circumstances: more than 200 governments are facing active COVID-19 cases and are using every power, resource and argument at their disposal to advance their interests — only some of which are directly related to COVID-19.

While an extraordinary range of technology-based COVID-19 proposals and ideas are emerging, as part of COVID-19 response, there are a specific group of biomedical and social control-focused projects requesting large amounts of historically and commercially regulated location data. There are five main categories of problems they strive to address:

- contact tracing;
- testing and responder capacity;
- early warning and surveillance;
- quarantine and social control; and
- research and cure.

These categories, and the analysis that follows, is necessarily painted with broad strokes. I’m choosing to focus on these problem categories — explicitly excluding important but secondary or tertiary categories, such as economic and social care infrastructure interventions and their effects, which deserve their own dedicated analysis.

More than 200 governments are facing active COVID-19 cases and are using every power, resource and argument at their disposal to advance their interests — only some of which are directly related to COVID-19.

What typically separates good from bad practice is adherence to rigorous, contextual testing and working within existing expertise, institutions and approaches to augment what we know works, rather than to work around or challenge the integrity of those experts or knowledge. We often forget, during times of great upheaval, how many of our quality assurances and basic rights protections are embedded in public institutional review. One of the unfortunate outcomes of emergency is that we temporarily suspend many of those systems, making it extremely difficult to determine whether the technology or data systems being proposed actually solve an important problem before we deploy them into vulnerable contexts. Still, most technology interventions won’t be successful enough to solve a problem, let alone become one themselves — but for those that do, their uses are relatively predictable. They are broadly used to increase awareness, capacity or cure. Viewed slightly differently, they are in service of either the biomedical response or the social and political controls used to limit transmission.

The goal is not to avoid using technology but to build on the ways that we know it works. And usually, technologies work in limited circumstances and based on specific, well-institutionalized understandings of response to make marginal increases in capacity. We also know these ways don’t typically require granting long-term, unchecked, open-ended emergency authorities. Here’s a bit more about the five categories of how technologies are typically deployed in response efforts, as well as some of the issues these uses raise.

Contact Tracing

Contact tracing is the process of tracking an epidemic’s spread — and by far the need to track the pathogen is the most common reason given to increase the amount of data shared during a public health emergency. Traditionally and institutionally, the way contact tracing works is that when a patient tests positive for COVID-19, they share as much about their recent whereabouts and contacts during the infectious period as possible. Here, what we know about how a disease travels — its transmission — is critical. If a disease can travel by air, being in the same space may matter — but if it requires you to exchange fluids, as Ebola does, then being in the same space isn’t as strong of an indicator. Public health professionals don’t always know how a disease travels, exactly, as is the case with COVID-19 — but they locate and test as many contacts as possible and, for the ones who test positive, repeat the process. The two most important things about the traditional approach to contact tracing are that it is based on specific knowledge — a positive test — not on probabilistic models, and that it’s directly tied to institutional response, so that it doesn’t alarm people to a risk without a clear pathway to treatment. The primary value of contact tracing is that it significantly accelerates individual and system awareness, testing and treatment.

The COVID-19 response is taking this traditional approach, but with the aid of technology — already the United States, Israel, Belgium, Pakistan and Austria have all proposed using call detail records in their contact-tracing strategies. Similarly, China and South Korea are receiving positive coverage for their uses of mobile technologies — in their enforcement of quarantine measures and as self-reporting symptom trackers, respectively. Predictably, there are also a growing number of civil society and private sector actors, often with the best of intentions, building or launching self-tracking and community notification applications, as a way of empowering communities to take control of their own response.

Contact tracing — as vitally important as it is — has a huge impact on people’s lives, as does the presumption of illness. Institutional approaches to contact tracing rely on medically approved tests, not only because public health institutions are reactive by design, but because the impacts are only acceptable if they’re based on facts. All of the approaches described above come with serious, societal risks. The use of mobile phone network data, for example, creates very granular, real-time targeting opportunities, which is dangerous for a number of reasons — as an illustration, in Israel, the government has said it will use location data to impose quarantine as a “requirement” that the government will enforce “without compromise.” Similarly, communities largely don’t have the awareness or tools to appropriately manage a response and can often give way to fear and discrimination. Problematically, broad public awareness ultimately doesn’t fix the primary determinant of COVID-19 mortality, which is health system capacity. And, of course, at a higher level, normalizing government-enforced, digitally delivered controls on our individual and collective rights creates the machinery for redeployment in future contexts, which may or may not be at this scale of emergency.
Testing and Responder Capacity

Another area where technology is applied in disaster response is to improve, adapt or invest in medical devices, tests, and protective gear. The good news in this area of intervention, which is exceptionally broad, is that when it’s effective, it’s transformative. The bad news, of course, is that a lot of the efforts to change or augment institutional testing capacity do so by reducing the quality control or scientific integrity of the underlying process.

Efforts to improve existing capacity, however, are some of the most positive ways to intervene, because they have comparatively specific problems to solve (i.e., improving the quality of protective gear), existing pathways to distribution (that is, testing, manufacturing and logistical distribution infrastructure) and users with at least a high-level understanding of the underlying tool. In other words, these efforts, where they are bounded by existing relationships, infrastructure and systems, often do well.

And, as a result, the efforts to ramp up to solve the practical problems surrounding testing for COVID-19 and the creative problems surrounding the need for equipment have been some of the most inspirational parts of the response. For example, South Korea’s use of drive-through testing to limit transmission at health facilities and increase throughput is largely hailed as a success. A range of health services — notably, Ontario’s — are leveraging self-diagnosis and telemedicine to help control the number of patients appearing in health-care facilities. And, while it’s caused some intellectual property litigation, one group of Italian hospital staff is using 3-D printers to try and resolve respirator distribution and manufacturing shortfalls. Using technology in these ways has been specific, limited, and largely created with, and based on, public health institutions’ need. Of course, these inevitably need to be modified when public institutions understand the transmission of the pathogen and are able to effectively model it based on available data — all of which are still in process for COVID-19.

Early Warning and Surveillance

Early warning and surveillance to better understand the pathogen and monitor the outbreak are critical components of responding to any epidemic, but there are significant differences between disease surveillance and individual surveillance. Disease surveillance focuses on tracking the incidence of the disease and its path, which often coincides with temporarily tracking the people who catch or interact with a disease but, critically, only insofar as absolutely necessary to limit the spread of the virus. Disease surveillance is a critical component of any pandemic response — and COVID-19 has been no exception.

There are significant, positive examples of this type of work. For example, despite deeply political and problematic early reporting, most countries have invested aggressively in testing, openly reporting their caseload and capacities, and are mobilizing rapidly around other critical disease-tracking initiatives. That means that there’s increasingly robust public reporting about the comparative size and scale of the outbreak, for example, the WHO’s daily global situation reports and resource portal and the Centers for Disease Control and Prevention’s updated world map. A number of academic publishers and news outlets have made their content available for free, to help rapidly increase public knowledge and capacity. There are distributed computing efforts, such as Folding@home, which helps people to donate their computer processing power to contribute to coronavirus research. Similarly, a number of COVID-19 strains have been genomically sequenced with unprecedented speed — which helps researchers understand, for example, how long the virus may have been in each community and its spread. These efforts play a critical role in helping public health authorities gauge the scope of the epidemic and make recommendations about how to adequately respond.

Art by Ben Giles

Unfortunately, efforts to engage the public in tracking and understanding disease surveillance can fall prey to a range of unintended consequences. For example, based on the South Korean Government’s mobile application, there are a number of technology efforts being marketed to consumers as ways to self-track and self-report symptoms, promoted as contributing toward the public’s interest by highlighting and monitoring risk. Similarly, the Government’s online tracking maintains an open database of personally identifiable cases (albeit not by name), with location histories and current information. At the best of times, using any individual technology’s user base as a representative sample for public health risk presents significant bias issues. When paired with the kinds of panic, scarcity and desperation that often accompany emergencies, such use can have dangerous and unintended consequences.

COVID-19 presents in some patients with symptoms such as fever and cough that are common to many less serious illnesses, while others who are infected with the virus are largely asymptomatic, which means that symptom tracking is not a good indicator of total infection. There are also ransomware, spyware and malware programs masquerading as coronavirus tracking applications.

There’s nothing inherently bad about individual symptom tracking, but these efforts rarely account for gaps in expertise and often report ambiguously defined risk to the app’s user base, public authorities or the public. Further, using quasi-scientific approaches to testing and then communicating it as ambient risk — especially when health systems are nearing their viral containment and treatment capacities — not only makes it harder to effectively model the pathogen, but also creates a significant risk of unnecessarily overwhelming responders. We’ve already seen the beginnings of that kind of panic, with a number of countries instituting largely ineffective public health responses, such as travel bans.

Using a reduced scientific standard to assess risk as a probability creates more uncertainty than it resolves and contributes to the significant misinformation, disinformation and exploitation that happen during disasters. And we’re already seeing force overwhelm nuance in the way response measures are being implemented. The flaws in those information systems too often make it easy to blur the line between disease surveillance and population surveillance — and to overlap the very real, very concerning implications of using technology for the latter.

Quarantine and Social Control

Quarantine and social control are important elements of the human side of a pandemic response — they are, essentially, the way that public health institutions try to contain, limit and stop the spread of a pathogen by controlling the movement of people. More concerning, we’re also seeing law enforcement and militaries enforcing lockdown requirements with violence — already resulting in the death of a man seeking food in India. They are also an extremely sensitive element of the relationship between a population and its governments, so much so that most governments require exceptional permissions to impose this type of social control. Most of those protections predate the advent of modern technology and were the standard of care in an era before the breadth or the granularity of digitally enabled social control that’s possible today was even imagined.
The common assumption in technology conversations is that resistance must emanate from the privacy community, and so these conversations often miss far more common problems, such as weak quality testing, bad problem selection and significant changes in the balance of individual and government powers. The way that we enable, administer and check the exceptional surveillance and social powers that each government exerts to contain COVID-19, especially as implemented through technology systems, will frame an important part of the future of state power in a world with increasing emergencies.

The first and most staggering examples of technology-augmented quarantine for COVID-19 came from China. The initial quarantine in Wuhan of more than 50 million people was, at the time, unprecedented. Now, mere weeks later, it’s being used as a paradigm and rolled out at global scale. One of the hallmarks of international coverage of the Chinese government’s response was its focus on the use of technology — in the beginning, as a way to control the public narrative and later, through the country’s broadly integrated social tracking systems and an app that dictated quarantine.

The way that we enable, administer and check the exceptional surveillance and social powers that each government exerts to contain COVID-19, especially as implemented through technology systems, will frame an important part of the future of state power in a world with increasing emergencies.

As COVID-19 response ramps up around the world, a growing number of countries are implementing social controls that involve a range of enforcement mechanisms — from public recommendations all the way to military enforcement. Perhaps the most important, and often ignored, impact of technology-focused interventions in surveillance is to effectively disable any checks on the government using them — they can wield these tools with impunity, which is by design. The theory of emergency powers is to let governments act unfettered, but the presumption — and the due process checks typically placed on emergency powers — is that they will do so with a clear-eyed, balanced approach to understanding the public’s interest. While the risks and harms associated with digital surveillance are often framed as related to privacy, there are significantly larger issues that apply during a pandemic, such as the escalation of government powers. Those powers have already shut down thousands of businesses, closed borders all over the world and taken 500 million students out of school.

Critically, we don’t currently have the frameworks to understand the individual role of digital interventions — and, rightfully, COVID-19 involves whole-of-community responses, which are happening online and offline, with and without apps. It bears repeating, as well, that every successful containment site to date (China, South Korea, Singapore, Taiwan) made large investments in proactive public testing, response infrastructure and coordinated, authoritative public messaging — all of which are cited by experts as vital components of effective response.

There are several, broad categories of digital social control systems, which largely break down by deployment model:

- government seizure/sharing of data or data infrastructure collected through private, commercial technologies to track citizens, such as mobile networks sharing location data with governments in Israel, China, Italy, Germany, Austria and, potentially, the United States, or to deploy artificial intelligence to predict risk;
- public deployment of increasingly invasive, privately developed technology and data profiling tools, such as using facial recognition to profile people through masks, or using tools of foreign intelligence contractors for public health surveillance or to decide who gets access to a COVID-19 test;
- privately deployed or “open” technologies that enable communities to self-generate and report data, such as the Government of Singapore’s contact-tracing database; and
- the repurposing of disaster response systems to become a point of digital intervention for state systems, such as using vaccination efforts to advance the interests of digital identity programs.

While this list isn’t entirely complete, it’s broad enough to cover the main structures of technology use for quarantine and social control — all of which are relatively unchecked during an emergency.

COVID-19 has become an unprecedented modern global emergency, with an ever-rising number of countries taking extraordinary measures to respond to the virus — including real-time location tracking, using algorithmic models to risk-score residents and enforcing quarantine, sometimes backed by military authority. In recent years, technology companies and platforms have been eager partners in turning their machinery toward experimentation during humanitarian crises, and now COVID-19 surveillance is fast becoming an industry. And whereas disease surveillance happens, broadly, within the confines of medical ethics institutions, the technology enabling personal surveillance used in the name of quarantine and social control is unconstrained by established mechanisms for testing its quality or contextual applicability. And without any view into its black box tools, we have no way of understanding the underlying equity or due process rights they may impinge, or of assessing the legitimacy of the government using those powers. Using state control as a proxy for legitimacy is a dangerous behaviour from any government, during times of disaster or otherwise.

Of course, focusing on surveillance powers misses the point that these systems are largely deployed to control people. Pandemic quarantine and social control systems are a rare example of institutional responses that demonstrate the full life cycle of governmental power — from detection and monitoring all the way through to enforcement — with almost no due process. Ultimately, the harms resulting from the expansion of government and industry powers with fewer checks and balances don’t fit neatly into any one “rights” category. As with corruption, or any other abuse-of-power harm, focusing on the abuse of procedural rights can distract from the larger harms of the intended ends.

Despite most coverage focusing on privacy rights, for example, the more fundamental problem is that, in a lot of cases, the technology simply doesn’t solve an important problem. For example, while it makes sense for public health institutions to surveil the disease — and potentially even people — there’s very little that non-medical surveillance efforts are able to do with the information that someone has a disease. Focusing on increasing surveillance of a biomedical condition is a very different proposition than focusing on helping to connect community members with needs to other community members who can help. In other words, there’s no need to know a person’s health status if they can effectively and safely communicate what you can actually do for them. And, similarly, there’s very little need to “surveil” a community through indirect technologies if they’re able and willing to trust you.

On the other, and more inevitable, end of the spectrum, however, is that government powers, once created, rarely go away. More commonly, they get extended and repurposed for political means. In the United States, the PATRIOT Act — marking a landmark increase in public surveillance powers in the aftermath of the terrorist attacks of September 11, 2001 — is expected to be renewed with bipartisan support more than 19 years after its initial event. Worse, once these powers become institutionally and politically convenient, the typical definition of “emergency” shifts — the United States government, for example, currently has 23 declared emergencies, each of which comes with some grant of extraordinary power for the executive branch. As each of the world’s responding governments considers how it will ramp up its emergency powers to deal with COVID-19, it’s equally critical that it considers the checks, institutional contexts and sunset provisions necessary to ensure disaster response doesn’t become a one-way ratchet away from civil liberties.

Ultimately, the primary reason for concern about tech-led surveillance technologies isn’t the underlying technology — it’s that the way they’re deployed circumvents the quality and human protections embedded in our existing institutional and market structures, which are vital during times of extended emergency. In institutional contexts with high degrees of transparency, independent checks on the exercise of authority, and public support for the intended outcome — like containing a pandemic — is often widely popular. For example, during the 2015 outbreak of MERS (Middle East Respiratory Syndrome, which involved another species of coronavirus), the Government of South Korea used mobile phone location data to quarantine 17,000 people, a process that was widely popular and largely effective. But, if a government does not have its people’s trust — and in places with significant amounts of public distrust (more places than you may think, according to the 2020 Edelman Trust Barometer) — there is a large practical need to accompany surveillance powers and any other emergency powers with significant oversight that, at the least, performs basic quality, necessity, proportionality and due process analysis regularly.
Due process checks are, of course, not a technology design feature — nor are they really applicable to the significant number of private actors involved in COVID-19 response surveillance. The reason that civil liberties advocates have raised concerns around the presence of companies such as Palantir in disaster response is precisely because they are so often instrumentalized against vulnerable groups. That is also what is concerning about a development like Israel’s use of location data to contract trace COVID-19: on the one hand, it’s a legitimately conferred, constitutionally bound set of authorities; on the other, the tracing is happening in a place with active violent conflict. How you feel about that use of technology very likely mirrors how you feel about the Israeli government.

But, regardless of how you feel about any specific use of surveillance technologies, it is neither new nor politically radical to suggest that where they implicate exceptional powers, both the constitutional and contractual checks on those powers should include robust oversight, sunset clauses and provisions for remediation of disputes, before these powers are exercised.

Vaccine, Mitigation and Treatment Research

Vaccine, mitigation and treatment research are easily some of the most valuable, and the most mature, uses of technology to accelerate pandemic response. For all of the incremental gains available through contact tracing, containment and mitigation, the way that public health systems “end” pandemics is through vaccines, treatments and institutionalizing response. The COVID-19 response has been no exception — even with expedited trials, public health authorities estimate that it will be between 12 and 18 months before a vaccine is ready. That timeline isn’t because it will take that long to develop a plausible prototype — it’s because that’s how long it will take to ensure that whatever vaccine governments deploy doesn’t have dangerous, unintended side effects.

While technology may hold significant potential for abuse, contributing resources to regulated research is one of the safest and most valuable ways for companies and experts to use technology to contribute to the COVID-19 response.

The use of technology to accelerate scientific research into sustainable solutions for emerging pathogens is extraordinarily effective and, mostly, straightforward. There are a number of projects that involve private companies contributing research, processing or other valuable resources to medium- and long-term response efforts. IBM, for example, contributed the world’s largest supercomputer toward identifying chemicals that limit COVID-19 transmission. Similar to the Folding@home approach, a number of public and public-private initiatives are sharing their data, research and computation to develop genomic maps, treatments and vaccines for the COVID-19 pandemic. Beyond largely institutional partnerships, coronavirus research has also reinvested the global community in the open and collaborative science movements.

While technology may hold significant potential for abuse, contributing resources to regulated research is one of the safest and most valuable ways for companies and experts to use technology to contribute to the COVID-19 response. The primary reason for that safety is that there are robust market, legal and institutional checks triggered at every stage between the invention of a vaccine in a contained biomedical research environment and the globally institutionalized distribution of a pharmaceutical product.

Conclusion

In 2020, it’s time to move past binary conversations about the use of technology for the public interest — “public” and “good” are inherently political concepts, not guarantees. We’re far enough along to recognize that there’s tremendous value to be gained from effective use of technology, but that this value is realized by working through systems, not by “disrupting” them when we need them most. While our existing institutions have many and major flaws, they were almost all invented to solve even bigger problems, and circumventing public institutions ignores a lot of hard-won protections from lessons learned. And, it’s critical that we don’t limit the scope of conversations about the potential for harm to discussions of privacy — the use of technology can cause an enormous range of harms during disaster, from using ineffective tools to enabling sweeping abuses of power.

There’s an understandable urge to “do something” in any disaster, and an inspiring range of communities admirably rise to the challenge of providing critical support during times of emergency. Communities, too, are not unalloyed “good” — and the communities pushing to “open” large parts of response informatics sometimes forget that governance largely exists because communities do not inherently realize their best selves. The technology industry is no exception — it often means well and has incredible capacities — and there have been truly transformative uses of data, research sharing and integrated technology deployments throughout the COVID-19 response. If anything, the COVID-19 response has, both positively and negatively, illustrated the importance of using technologies to mobilize and coordinate response efforts.

This analysis has focused on the uses and abuses of technology interventions aimed directly at pandemic response — and intentionally excludes the systems and technologies involved in second-order effects, such as public communication, economic stimulus or law enforcement. And, perhaps predictably, where we end up is a recognition that access to technology can be valuable — but mostly when situated in need and exercised through institutional mechanisms to ensure contextual value, necessity and proportionality. In other words, when governed.

There is no shortage of inspirational stories emerging from the COVID-19 response — many of which involve the use of technology, but very few of which are driven by it. Emergencies, especially at a global scale, cause fear and, in many instances, truly awesome generosity. No matter your interpretation of the COVID-19 response, one thing should be universal: emergencies are not a blank cheque for state or digital platform power. And amid this historic, global investment in the international connections between our public health systems, it’s absolutely essential that we use technology to amplify institutional capacity and state powers — while we also invest in designing oversight and governance that appeal to established, global standards for the exercise of exceptional powers.

In times of emergency, with the best of intentions, people mobilize the best of their capacities to respond, and those capacities are increasingly digital. If we’re going to realize the value of those good intentions, we’ll need governance to ensure that the direction they pave serves us all.

The opinions expressed in this article/multimedia are those of the author(s) and do not necessarily reflect the views of CIGI or its Board of Directors.

About the Author
Sean McDonald

Sean Martin McDonald is a CIGI senior fellow and the co-founder of Digital Public, which builds legal trusts to protect and govern digital assets.