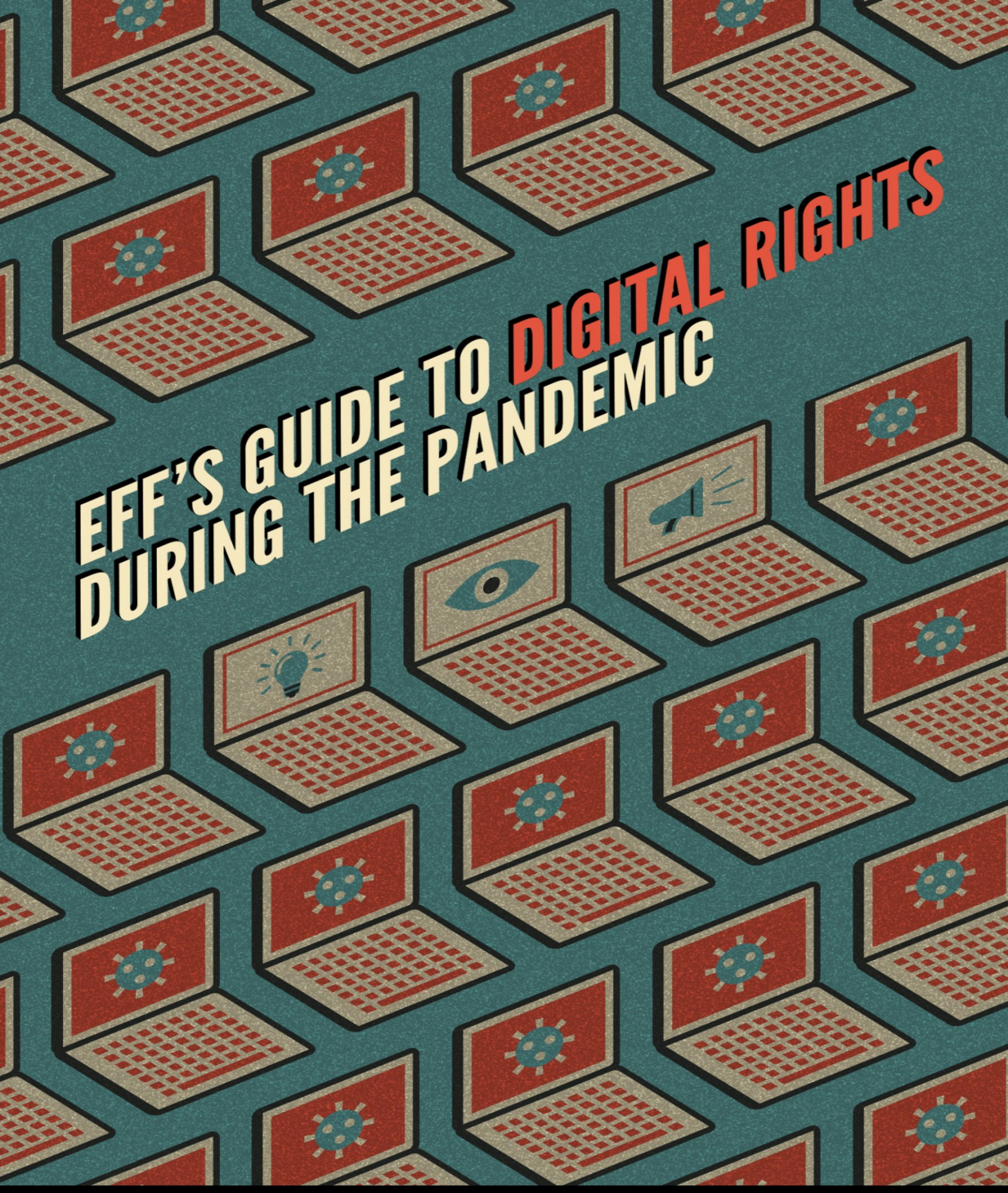


EFF

Table of Contents:

EFF's Guide to Digital Rights During the Pandemic:
The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, transparency, and innovation through impact litigation, activism, and technology. For more information, visit eff.org. For more information on COVID-19 and digital rights, visit eff.org/issues/covid-19.

EFF's Guide to Digital Rights During the Pandemic
Published May 4, 2020
ISBN 978-0-9966686-7-5

Editing: Jason Kelley
Cover art: Hugh D'Andrade
Formatting: Tobias S. Buckell
Legal: Adam Schwartz, David Greene, Naomi Gilens, Saira Hussain

With Assistance and Writing by:
Cindy Cohn, Danny O'Brien, Matthew Guariglia, Jillian York, Elliot Harmon, Jacob Hoffman-Andrews, Ernesto Falcon, Gennie Gebhart, Dave Maass, Mark Rumold, Rory Mir, Katharine Trendacosta, Corynne McSherry, Lindsay Oliver, Daly Barnett, Kit Walsh, Cory Doctorow, Sophia Cope, Kurt Opsahl, Bennett Cyphers, Andrew Crocker, Cooper Quintin, Hayley Tsukayama, Soraya Okuda, Will Greenberg, Ben Elam, Alex Moss

Please support our work and spread the word about this collection.
https://www.eff.org/pandemicguide

Electronic Frontier Foundation
815 Eddy. St
San Francisco, CA 94115
415-436-9333 / info@eff.org

Facing the Exponential

At EFF we've long been accustomed to scrutinizing the ruthless logic of the exponential curve. For the majority of our organization's existence, the curve was Moore's Law: the constant doubling of computer power every eighteen months, more or less, that determined the path of digital progress. We learned from those times that it made no sense to anchor our work of defending civil liberties to the incidental technicalities of the present, no matter how up-to-the-minute or futuristic they might seem to be. Regulations that expected video-recorders, fax machines or e-mail to be the last word in high tech advances, society-wide mandates that depended on soon-to-be-broken algorithms or rapidly-evaporating business models: there is nothing that is less resilient or protective of long-term human values than statements grounded only in today's hot tech take. The iron law of the exponential curve would just blow those assumptions away.

To envisage and defend a high-tech society that still protected civil liberties, our lawyers, activists and technologists have learned instead to face those logarithmic precipices together, seeking out the constants, and the constraints. Principles that could tie human rights and technology together for the long term: norms that would survive decades not days, and on whose firm foundation we could set in place, in a timely fashion, laws and standards that would see our open society through precipitous times ahead.

The rapid exponential change we face now comes not from the pace of modern innovation, but from the starker, crueler mathematics of a pandemic. The numbers marked out on this curve are not transistors per square centimeter, but human lives. In these times,

once again, our greatest risk is for policy-makers and technologists to become locked into the velocity of the moment: reacting to the daily disruptive threats as they happen, without regard to the warnings of the past, or extrapolating the predictable consequences of their actions upon the future.

To plan just for the moment while being hurled up an exponential curve, as we have already seen at the cost of thousands of lives, is to react both too weakly, and too late.

This book on the interactions between COVID-19 and technology was written by our teams of lawyers, technologists, activists and experts, at an extraordinary pace in the first few weeks of the United States' COVID-19 shut-down. Despite that swiftness, its conclusions have been built on years of preparative work. In those weeks, we wrote multiple blog posts a day, not just to be timely, but to assemble our own thoughts on the changing situation: to try and inject dependable, timeless concerns when they most need to be heard. While the articles were written to speak to policymakers and citizens at the moment that they were first reacting to the new realities of the virus, they are not "hot takes." They were all written with an explicit eye to what lay beyond the exponential curve, based on our experience tangling with rapid societal and technological change in earlier years.

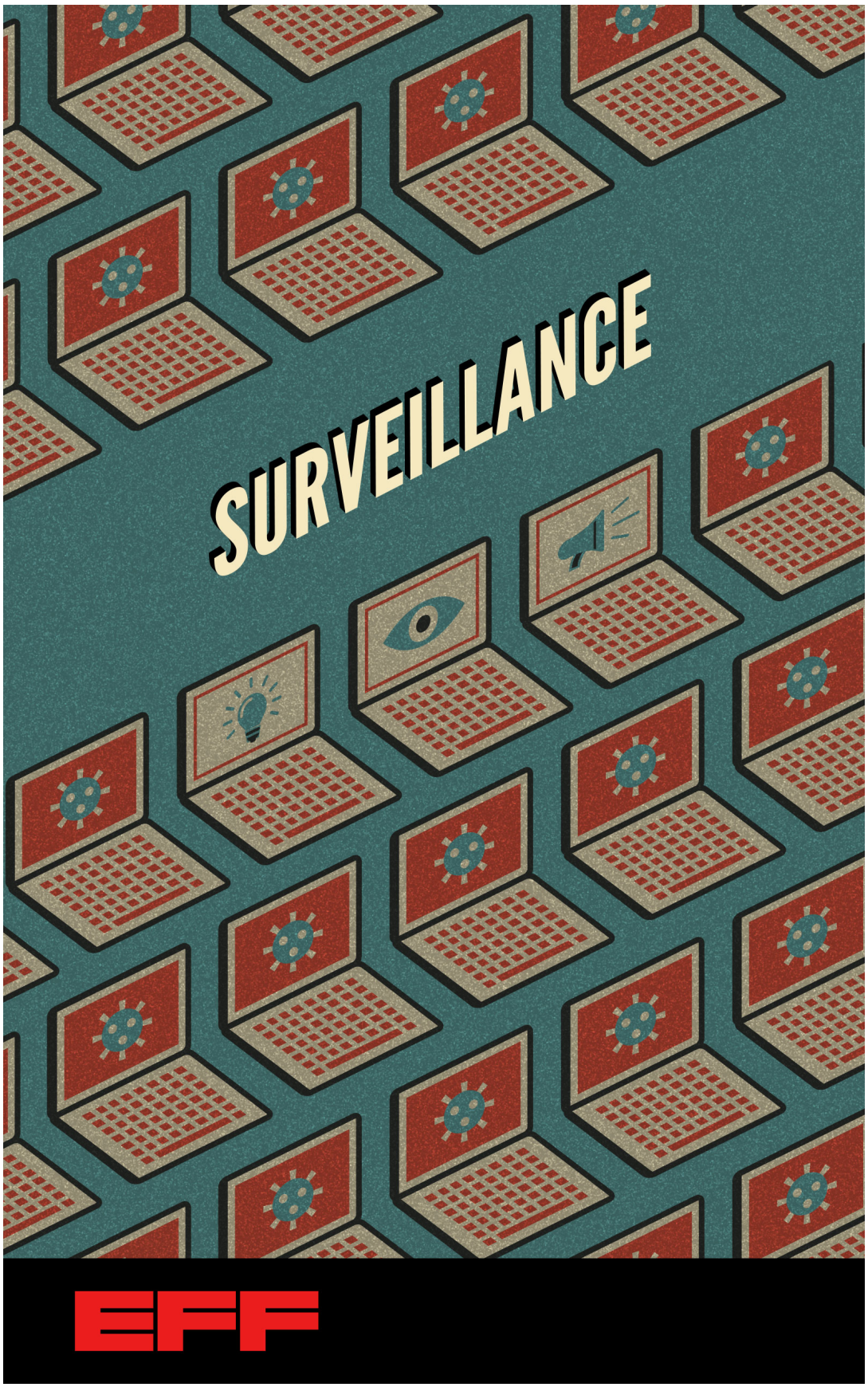
This short book collects those conclusions together. Ubiquitous location tracking and surveillance cameras, for example, would create an infrastructure of state surveillance without a firm footing in human rights principles. Here you'll find those principles spelled out in detail. Companies and innovators have stepped up to let us live as best a life as we can under quarantine, but often by being careless with their users' privacy and security. These tools themselves need to

be treated with careful hygiene protocols, listed here. Companies and states have already been tempted to flip the "censorship" switch and treat free expression as another viral threat: but we demonstrate that whistleblowers and critics have already saved lives in this pandemic. If we are to save more lives, their voices must be heard, and their anonymity or pseudonymity protected. When existing systems failed, mutual aid has helped millions: but the modern tools of support networks have their own privacy challenges, which we spell out here. The speed of the coronaviruses' rise meant that only the rapid, self-organizing, and global co-ordinating abilities of an open Internet filled with open access and open science could ever have hoped to keep up, let alone lead the way to finding robust treatments and best medical practices. But this public interest Internet cannot survive without active support—support that should be forthcoming in the economically troubled times ahead. We have some ideas of what that support should look like: and it's not a bail-out for big tech or the telecoms.

It's the nature of an exponential—even one aggressively dampened by policy, science and technology—that the threat will not relent, at least until a permanent cure can put COVID-19 behind us. But we hope that the firm grounding of precedent, principle and a deep understanding of the promise and limits of technological solutions to this crisis mean that this book will be useful not only at its time of writing, but also on the other side of the curve.

It's hard to predict the future when you stand beneath the cliff-face of an exponential. But we must try. We look forward to seeing you over there, in a future made better for us all.

If you find this guide useful, please consider joining the force for good that makes it possible: our membership. Your donation will go directly to supporting EFF's thirty-year mission—to ensure that technology supports freedom, justice, and innovation for all the people of the world. Join us at https://www.eff.org/pandemicguide, and keep up to date with our writing on technology, COVID-19 and much more at https://www.eff.org/.


SURVEILLANCE
EFF

SECTION 1: SURVEILLANCE

Governments around the world are demanding extraordinary new surveillance powers intended to contain the virus' spread, often in partnership with corporations that hold vast stores of consumers' personal data. Many proposals would invade our privacy, deter our free speech, and disparately burden vulnerable groups of people. As expanded upon in this guide, we at EFF ask three questions when analyzing proposals that would provide greater surveillance powers to the government: Would the proposal work? Would it excessively intrude on our freedoms? And are there sufficient safeguards?

Different proposals raise different issues. For example:

- Government has not shown that some intrusive technologies would work, such as phone location surveillance, which is insufficiently granular to identify when two people were close enough together to transmit the virus.
- Some technologies are too dangerous to a democratic society, such as dragnet surveillance cameras that use face recognition or thermal imaging.
- Some technologies need strict safeguards, such as aggregate location data used to inform public health decisions.

As public health authorities are working to contain the spread of COVID-19, many government agencies are collecting and analyzing personal information about large numbers of identifiable people, including their health, travel, and personal relationships. As our society struggles with how best to minimize the spread of this disease, we must carefully consider the way that "big data" containment tools impact our digital liberties.

EFF has long advocated against digital surveillance by governments and corporations of our movements, health, and personal relationships, and against big data systems that can turn our lives into open books. Such data processing often invades our privacy, deters our free speech and association, and disparately burdens communities of color. Any use of personal data must be medically necessary; any new processing of personal data must be proportionate to the actual need; people must not be scrutinized because of their nationality or other demographic factors; and any new government powers must expire when the disease is contained.

Glossary

Contact tracing: This is the long-standing public health process of identifying who an infected person may have come into contact with while they were contagious. In traditional or **manual contact tracing**, healthcare workers interview an infected individual to learn about their movements and people with whom they have been in close contact. Healthcare workers then reach out to the infected person's potential contacts, and may offer them help, or ask them to self-isolate and get a test, treatment, or vaccination if available.

Digital contact tracing: Some companies, governments, and others are experimenting with using smartphone apps to complement public health workers' contact tracing efforts. Most implementations focus on **exposure notification:** notifying a user that they have been near another user who's been diagnosed positive, and getting them in contact with public health authorities. Additionally, these kinds of apps—which tend to use either **location tracking** or **proximity tracking**—can only be effective in assisting the fight against COVID-19 if there is also widespread testing and interview-based contact tracing. Even then, they might not help much. Among other concerns, any app-based or smartphone-based solution will systematically miss groups least likely to have a smartphone and *most* at risk of COVID-19: in the United States, that includes elderly people, low-income households, and rural communities.

Contact tracing using location tracking: Some apps propose to determine which pairs of people have been in contact with each other

by collecting location data (including GPS data) for all app users, and looking for individuals who were in the same place at the same time. But location tracking is **not** well-suited to contact tracing of COVID-19 cases. Data from a mobile phone's GPS or from cell towers is simply not accurate enough to indicate whether two people came into close physical contact (i.e. within 6 feet). But it *is* accurate enough to expose sensitive, individually identifiable information about a person's home, workplace, and routines.

Contact tracing using proximity tracking: Proximity tracking apps use Bluetooth Low Energy (BLE) to determine whether two smartphones are close enough for their users to transmit the virus. BLE measures proximity, not location, and thus is better suited to contact tracing of COVID-19 cases than GPS or cell site location information. When two users of the app come near each other, both apps estimate their proximity using Bluetooth signal strength. If the apps estimate that they are less than approximately six feet apart for a sufficient period of time, the apps exchange identifiers. Each app logs an encounter with the other's identifier. When a user of the app learns that they are infected with COVID-19, other users can be notified of their own infection risk. Many different kinds of proximity tracking apps have been built and proposed. For example, Apple and Google have announced plans for an API to allow developers to build this kind of app.

How EFF Evaluates Government Demands for New Surveillance Powers

The COVID-19 public health crisis has no precedent in living memory. But government demands for new high-tech surveillance powers are all too familiar. This includes well-meaning proposals to use various forms of data about disease transmission among people. Even in the midst of a crisis, the public must carefully evaluate such government demands, because surveillance invades privacy, deters free speech, and unfairly burdens vulnerable groups. It also metastasizes behind closed doors. And new surveillance powers tend to stick around. For example, nearly two decades after the 9/11 attacks, the NSA is still conducting dragnet Internet surveillance.

When governments demand new surveillance powers—especially now, in the midst of a crisis like the ongoing COVID-19 outbreak—EFF always asks these questions:

- First, has the government shown its surveillance would be effective at solving the problem?
- Second, if the government shows efficacy, we ask: Would the surveillance do too much harm to our freedoms?
- Third, if the government shows efficacy, and the harm to our freedoms is not excessive, we ask: Are there sufficient guardrails around the surveillance?

Would It Work?

The threshold question is whether the government has shown that its surveillance plan would be effective at solving the problem at hand. This must include published details about what the government

plans, why this would help, and what rules would apply. Absent efficacy, there is no reason to advance to the next questions. Surveillance technology is always a threat to our freedoms, so it is only justified where (among other things) it would actually do its job.

Sometimes, we simply can't tell whether the plan would hit its target. For example, governments around the world are conducting location surveillance with phone records, or making plans to do so, in order to contain COVID-19. Governments so far haven't shown this surveillance works.

Would It Do Too Much Harm?

Even if the government shows that a surveillance power would be effective, we still oppose its use if it would too greatly burden our freedoms. High-tech surveillance can turn our lives into open books. It can chill and deter our participation in protests, advocacy groups, and online forums. Its burdens fall all too often on people of color, immigrants, and other vulnerable groups. Breaches of government data systems can expose intimate details about our lives to scrutiny by adversaries including identity thieves, foreign governments, and stalkers. In short, even if surveillance would be effective at solving a problem, it must also be, as international human rights law dictates, necessary and proportionate to that problem, and not have an outsized impact on vulnerable groups.

Thus, for example, EFF opposes NSA dragnet Internet surveillance, even if it can theoretically provide leads to uncovering terrorists, such as the proverbial needle in the haystack. We believe this sort of mass, suspicionless surveillance is simply incompatible with universal human rights. Similarly, we oppose face surveillance, even

if this technology sometimes contributes to solving crime. The price to our freedoms is simply too great.

On the other hand, the United States' Centers for Disease Control and Protection (CDC) program for contact tracing of international flights, proposed in February 2020 as an amendment to their standard quarantine regulations, might be necessary and proportionate. It would require airlines to maintain the names and contact information of passengers and crews arriving from abroad. If a person on a flight turned out to be infected, the program would then require the airline to send the CDC the names and contact information of the other people on the flight. This program applies to a discrete set of information about a discrete set of people. It will only occasionally lead to disclosure of this information to the government. And it is tailored to a heightened transmission risk: people returning from a foreign country, who are densely packed for many hours in a sealed chamber. However, as we wrote at the time , it is unclear to us whether this program has sufficient safeguards.

Are the Safeguards Sufficient?

Even if the government shows a form of high-tech surveillance is effective, and even if such surveillance would not intolerably burden our freedoms, EFF still seeks guardrails to limit whether and how the government may conduct this surveillance. These include, in the context of surveillance for public health purposes:

1. ***Consent***. For reasons of both personal autonomy and effective public health response, people should have the power to decide whether or not to participate in surveillance systems, such as an app

built for virus-related location tracking. Such consent must be informed, voluntary, specific, and opt-in.

2. Minimization. Surveillance programs must collect, retain, use, and disclose the least possible amount of personal information needed to solve the problem at hand. For example, information collected for one purpose must not be used for another purpose, and must be deleted as soon as it is no longer useful to the original purpose. In the public health context, it may often be possible to engineer systems that do not share personal information with the government. When the government has access to public health information, it must not use it for other purposes, such as enforcement of criminal or immigration laws.

3. Information security. Surveillance programs must process personal information in a secure manner, and thereby minimize risk of abuse or breach. Robust security programs must include encryption, third-party audits, and penetration tests. And there must be transparency about security practices.

4. Privacy by design. Governments that undertake surveillance programs, and any corporate vendors that help build them, must employ privacy officers, who are knowledgeable about technology and privacy, and who ensure privacy safeguards are designed into the program.

5. Community control. Before a government agency uses a new form of surveillance, or uses a form of surveillance it has already ac-

quired in a new way, it must first obtain permission from its legislative authority, including approval of the agency's proposed privacy policy. The legislative authority must consider community input based on the agency's privacy impact report and proposed privacy policy.

6. Transparency. The government must publish its policies and training materials, and regularly publish statistics and other information about its use of each surveillance program in the greatest detail possible. Also, it must regularly conduct and publish the results of audits by independent experts about the effectiveness and any misuse of each program. Further, it must fully respond to public records requests about its programs, taking into account the privacy interests of people whose personal information has been collected.

7. Anti-bias. Surveillance must not intentionally or disparately burden people on the basis of categories such as race, ethnicity, religion, nationality, immigration status, LGBTQ status, or disability.

8. Expression. Surveillance must not target, or document information about, people's political or religious speech, association, or practices.

9. Enforcement. Members of the community must have the power to go to court to enforce these safeguards, and evidence collected in violation of these safeguards must be excluded from court proceedings.

10. ***Expiration***. If the government acquires a new surveillance power to address a crisis, that power must expire when the crisis ends. Likewise, personal data that is collected during the crisis, and used to help mitigate the crisis, must be deleted or minimized when the crisis is over. And crises cannot be defined to last in perpetuity.

Outside the context of public health, surveillance systems need additional safeguards. For example, before using a surveillance tool to enforce criminal laws, the government must first obtain a warrant from a judge, based on probable cause that evidence of a crime or contraband would be found, and particularly describing who and what may be surveilled. Targets of such surveillance must be promptly notified, whether or not they are ever prosecuted. Additional limits are needed for more intrusive forms of surveillance: use must be limited to investigation of serious violent crimes, and only after exhaustion of less intrusive investigative methods.

Conclusion

Once the genie is out of the bottle, it is hard to put back. That's why we ask these questions about government demands for new high-tech surveillance powers, especially in the midst of a crisis. Has the government shown it would be effective? Would it do too much harm to our freedoms? Are there sufficient guardrails?

Governments Haven't Shown Location Surveillance Would Help Contain COVID-19

Governments around the world are demanding new dragnet location surveillance powers to contain the COVID-19 outbreak. But before the public allows their governments to implement such systems, governments must explain to the public how these systems would be effective in stopping the spread of COVID-19. There's no questioning the need for far-reaching public health measures to meet this urgent challenge, but those measures must be scientifically rigorous, and based on the expertise of public health professionals.

Governments have not yet met that standard, nor even shown that extraordinary location surveillance powers would make a significant contribution to containing COVID-19. Unless they can, there's no justification for their intrusions on privacy and free speech, or the disparate impact these intrusions would have on vulnerable groups. Indeed, governments have not even been transparent about their plans and rationales.

The Costs of Location Surveillance

EFF has long opposed location surveillance programs that can turn our lives into open books for scrutiny by police, surveillance-based advertisers, identity thieves, and stalkers. Many sensitive inferences can be drawn from a visit to a health center, a criminal defense lawyer, an immigration clinic, or a protest planning meeting.

Moreover, fear of surveillance chills and deters free speech and association. And all too often, surveillance disparately burdens peo-

ple of color. What's more, whatever personal data collected by government can be misused by its employees, stolen by criminals and foreign governments, and unpredictably redirected by agency leaders to harmful new uses.

Emerging Dragnet Location Surveillance

China responded to the COVID-19 crisis by building new infrastructures to track the movements of massive numbers of identifiable people. Israel tapped into a vast trove of cellphone location data to identify people who came into close contact with known virus carriers. That nation has sent quarantine orders based on this surveillance. About a dozen countries are reportedly testing a spy tool built by NSO Group that uses huge volumes of cellphone location data to match the location of infected people to other people in their vicinity (NSO's plan is to not share a match with the government absent such a person's consent).

Disturbingly, most of the public information about government's emerging location surveillance programs comes from anonymous sources, and not official explanations. Transparency is a cornerstone of democratic governance, especially now, in the midst of a public health crisis. If the government is considering such new surveillance programs, it must publicly explain exactly what it is planning, why this would help, and what rules would apply. History shows that when government builds new surveillance programs in secret, these programs quickly lead to unjustified privacy abuses. That's one reason EFF has long demanded transparent democratic control over whether government agencies may deploy new surveillance technology.

Governments Must Show Their Work

Because new government dragnet location surveillance powers are such a menace to our digital rights, governments should not be granted these powers unless they can show the public how these powers would actually help, in a significant manner, to contain COVID-19. Even if governments could show such efficacy, we would still need to balance the benefit of the government's use of these powers against the substantial cost to our privacy, speech, and equality of opportunity. And even if this balancing justified government's use of these powers, we would still need safeguards, limits, auditing, and accountability measures. In short, new surveillance powers must always be necessary and proportionate.

But today, we can't balance those interests or enumerate necessary safeguards, because governments have not shown how the proposed new dragnet location surveillance powers could help contain COVID-19. The following are some of the points we have not seen the government publicly address.

1. Are the location records sought sufficiently granular to show whether two people were within transmittal distance of each other? In many cases, we question whether such data will actually be useful to healthcare professionals.

This may seem paradoxical. After all, location data is sufficiently precise for law enforcement to place suspects at the scene of a crime, and for juries to convict largely on the basis of that evidence. But when it comes to tracking the spread of a disease that requires close personal contact, data generated by current technology generally

can't reliably tell us whether two people were closer than the CDC-recommended radius of six feet for social distancing.

For example, cell site location information (CSLI)—the records generated by mobile carriers based on which cell towers a phone connects to and when—is often only able to place a phone within a zone of half a mile to two miles in urban areas. The area is even wider in areas with less dense tower placement. GPS sensors built directly into phones can do much better, but even GPS is only accurate to a 16-foot radius. These and other technologies like Bluetooth can be combined for better accuracy, but there's no guarantee that a given phone can be located with six-foot precision at a given time.

2. Do the cellphone location records identify a sufficiently large and representative portion of the overall population? Even today, not everyone has a cellphone, and some people do not regularly carry their phones or connect them to a cellular network. The population that carries a networked phone at all times is not representative of the overall population; for example, people without phones skew towards lower-income people and older people.

3. Has the virus already spread so broadly that contact tracing is no longer a significant way to reduce transmission? If community transmission is commonplace, contact tracing may become impractical or divert resources from more effective containment methods.

4. Will health-based surveillance deter people from seeking health care? Already, there are reports that people subject to

COVID-based location tracking are altering their movements to avoid embarrassing revelations. If a positive test result will lead to enhanced location surveillance, some people may avoid testing.

Conclusion

As our society struggles with COVID-19, far narrower "big data" surveillance proposals may emerge. Perhaps public health professionals will show that such proposals are necessary and proportionate. If so, EFF would seek safeguards, including mandatory expiration when the health crisis ends, independent supervision, strict anti-discrimination rules, auditing for efficacy and misuse, and due process for affected people.

But for now, the government has not shown that new dragnet location surveillance powers would significantly help to contain COVID-19. It is the government's job to show the public why this would work.

How to Protect Privacy When Aggregating Location Data to Fight COVID-19

As governments, the private sector, NGOs, and others mobilize to fight the COVID-19 pandemic, we've seen calls to use location information—typically drawn from GPS and cell tower data—to inform public health efforts. Among the proposed uses of location data, one of the most widely discussed is analyzing aggregated data about which locations people are visiting, whether they are traveling less, and other collective measurements of individuals' movement. This analysis might be used to inform judgments about the effectiveness of shelter-in-place orders and other social distancing measures. Projects making use of aggregated location data have graded residents of each state on their social distancing and visualized the travel patterns of people on returning from spring break. Most recently, Google announced that it would publish ongoing "COVID-19 Community Mobility Reports," which draw on the company's store of location data to report on changes at a community level in people's travel to various locations such as grocery stores, parks, and mass transit stations.

Compared to using individualized location data for contact tracing—as many governments around the world are already doing—deriving public health insights from aggregated location data poses far fewer privacy and other civil liberties risks such as restrictions on freedom of expression and association. However, even "aggregated" location data comes with potential pitfalls. This post discusses those pitfalls and describes some high-level best practices for those who seek to use aggregated location data in the fight against COVID-19.

What Does "Aggregated" Mean?

At the most basic level, there's a difference between "aggregated" location data and "anonymized" or "deidentified" location data. Practically speaking, there is no way to deidentify individual location data. Information about where a person is and has been itself is usually enough to reidentify them. Someone who travels frequently between a given office building and a single-family home is probably unique in those habits and therefore identifiable from other readily identifiable sources. One widely cited study from 2013 even found that researchers could uniquely characterize 50% of people using only two *randomly* chosen time and location data points.

Aggregation to preserve individual privacy, on the other hand, can potentially be useful. Aggregating location data involves producing counts of behaviors instead of detailed timelines of individual location history. For instance, an aggregation might tell you how many people's phones reported their location as being in a certain city within the last month. Or it might tell you, for a given area in a city, how many people traveled to that area during each hour in the last month. Whether or not a given scheme for aggregating location data works to improve privacy depends deeply on the details: On what timescale is the data aggregated? How large of an area does each count cover? When is a count considered too low and dropped from the data set?

For example, Facebook uses differential privacy techniques such as injecting statistical noise into the dataset as part of the methodology of its "Data for Good" project. This project aggregates Facebook users' location data and shares it with various NGOs, academics, and

governments engaged in responding to natural disasters and fighting the spread of disease, including COVID-19.

There is no single magic formula for aggregating individual location data such that it provides insights that might be useful for some decisions and yet still cannot be reidentified. Instead, it's a question of tradeoffs. As a matter of public policy, it is critical that user privacy not be sacrificed when creating aggregated location datasets to inform decisions about COVID-19 or anything else.

How Do We Evaluate the Use of Aggregated Location Data to Fight COVID-19?

Because aggregation reduces the risk of revealing intimate information about individuals' lives, we are less concerned about this use of location data to fight COVID-19 compared to individualized tracking. Of course, the choice of the aggregation parameters generally needs to be done by domain experts. As in the Facebook and Google examples above, these experts will often be working within private companies with proprietary access to the data. Even if they make all the right choices, the public needs to be able to review these choices because the companies are sharing the *public's* data. For the experts doing the aggregation, there's often pressure to reduce the privacy properties in order to generate an aggregate data set that a particular decision-maker claims must be more granular in order to be meaningful to them. Ideally, companies would also consult outside experts before moving forward with plans to aggregate and share location data. Getting public input on whether a given data-sharing scheme sufficiently preserves privacy can help reduce the bias that such pressure creates.

As a result, companies like Google that produce reports based on aggregated location data from users should release their full methodology as well as information about who these reports are shared with and for what purpose. To the extent they only share certain data with selected "partners," these groups should agree not to use the data for other purposes or attempt to re-identify individuals whose data is included in the aggregation. And, as Google has already done, companies should pledge to end the use of this data when the need to fight COVID-19 subsides.

For any data sharing plan, consent is critical: Did each person consent to the method of data collection, and did they consent to the use? Consent must be specific, informed, opt-in, and voluntary. Ordinarily, users should have the choice of whether to opt-in to every new use of their data, but we recognize that obtaining consent to aggregate previously acquired location data to fight COVID-19 may be difficult with sufficient speed to address the public health need. That's why it's especially important that users should be able to review and delete their data at any time. The same should be true for anyone who truly consents to the collection of this information. Many entities that hold location information, like data brokers that collect location from ads and hidden tracking in apps, can't meet these consent standards. Yet many of the uses of aggregated location data that we've seen in response to COVID-19 draw from these tainted sources. At the very least, data brokers should not profit from public health insights derived from their stores of location data, including through free advertising. Nor should they be allowed to "COVID wash" their business practices: the existence of these data

stores is unethical, and should be addressed with new consumer data privacy laws.

Finally, we should remember that location data collected from smartphones has limitations and biases. Smartphone ownership remains a proxy for relative wealth, even in regions like the United States where 80% of adults have a smartphone. People without smartphones tend to already be marginalized, so making public policy based on aggregate location data can wind up disregarding the needs of those who simply don't show up in the data, and who may need services the most. Even among the people with smartphones, the seeming authoritativeness and comprehensiveness of large-scale data can cause leaders to reach erroneous conclusions that overlook the needs of people with fewer resources. For example, data showing that people in one region are traveling more than people in another region might not mean, as first appears, that these people are failing to take social distancing seriously. It might mean, instead, that they live in an underserved area and must thus travel longer distances for essential services like groceries and pharmacies.

In general, our advice to organizations that consider sharing aggregate location data: Get consent from the users who supply the data. Be cautious about the details. Aggregate on the highest level of generality that will be useful. Share your plans with the public before you release the data. And avoid sharing "deidentified" or "anonymized" location data that is not aggregated—it doesn't work.

The Challenge of Proximity Apps For COVID-19 Contact Tracing

Around the world, a diverse and growing chorus is calling for the use of smartphone proximity technology to fight COVID-19. In particular, public health experts and others argue that smartphones could provide a solution to an urgent need for rapid, widespread contact tracing—that is, tracking who infected people come in contact with as they move through the world. Proponents of this approach point out that many people already own smartphones, which are frequently used to track users' movements and interactions in the physical world.

But it is not a given that smartphone tracking will solve this problem, and the risks it poses to individual privacy and civil liberties are considerable. *Location tracking*—using GPS and cell site information, for example—is not suited to contact tracing because it will not reliably reveal the close physical interactions that experts say are likely to spread the disease. Instead, developers are rapidly coalescing around applications for *proximity tracing*, which measures Bluetooth signal strength to determine whether two smartphones were close enough together for their users to transmit the virus. In this approach, if one of the users becomes infected, others whose proximity has been logged by the app could find out, self-quarantine, and seek testing. Apple and Google have announced joint application programming interfaces (APIs) using these principles that will be rolled out in iOS and Android in May 2020. A number of similarly designed applications are also being prepared.

As part of the nearly unprecedented societal response to COVID-19, such apps raise difficult questions about privacy, efficacy, and responsible engineering of technology to advance public health. Above all, we should not trust any application—no matter how well-designed—to solve this crisis or answer all of these questions. Contact tracing applications cannot make up for shortages of effective treatment, personal protective equipment, and rapid testing, among other challenges.

COVID-19 is a worldwide crisis, one which threatens to kill millions and upend society, but history has shown that exceptions to civil liberties protections made in a time of crisis often persist much longer than the crisis itself. With technological safeguards, sophisticated proximity tracking apps may avoid the common privacy pitfalls of location tracking. Developers and governments should also consider legal and policy limits on the use of these apps. Above all, the choice to use them should lie with individual users, who should inform themselves of the risks and limitations, and insist on necessary safeguards. Some of these safeguards are discussed below.

How Do Proximity Apps Work?

There are many different proposals for Bluetooth-based proximity tracking apps, but at a high level, they begin with a similar approach. The app broadcasts a unique identifier over Bluetooth that other, nearby phones can detect. To protect privacy, many proposals, including the Apple and Google APIs, rotate each phone's identifier frequently to limit the risk of third-party tracking.

When two users of the app come near each other, both apps estimate the distance between each other using Bluetooth signal

strength. If the apps estimate that they are less than approximately six feet (or two meters) apart for a sufficient period of time, the apps exchange identifiers. Each app logs an encounter with the other's identifier. The users' location is not necessary, as the application need only know if the users are sufficiently close together to create a risk of infection.

When a user of the app learns that they are infected with COVID-19, other users can be notified of their own infection risk. This is where different designs for the app significantly diverge.

Some apps rely on one or more central authorities that have privileged access to information about users' devices. For example, TraceTogether, developed for the government of Singapore, requires all users to share their contact information with the app's administrators. In this model, the authority keeps a database that maps app identifiers to contact information. When a user tests positive, their app uploads a list of all the identifiers it has come into contact with over the past two weeks. The central authority looks up those identifiers in its database, and uses phone numbers or email addresses to reach out to other users who may have been exposed. This places a lot of user information out of their own control, and in the hands of the government. This model creates unacceptable risks of pervasive tracking of individuals' associations and should not be employed by other public health entities.

Other models rely on a database that doesn't store as much information about the app's users. For example, it's not actually necessary for an authority to store real contact information. Instead, infected users can upload their contact logs to a central database, which stores anonymous identifiers for everyone who may have been

exposed. Then, the devices of users who are not infected can regularly ping the authority with their own identifiers. The authority responds to each ping with whether the user has been exposed. With basic safeguards in place, this model could be more protective of user privacy. Unfortunately, it may still allow the authority to learn the real identities of infected users. With more sophisticated safeguards, like cryptographic mixing, the system could offer slightly stronger privacy guarantees.

Some proposals go further, publishing the entire database publicly. For example, Apple and Google's proposal, published April 10, would broadcast a list of keys associated with infected individuals to nearby people with the app. This model places less trust in a central authority, but it creates new risks to users who share their infection status that must be mitigated or accepted.

Some apps require authorities, like health officials, to certify that an individual is infected before they may alert other app users. Other models could allow users to self-report infection status or symptoms, but those may result in significant numbers of false positives, which could undermine the usefulness of the app.

In short, while there is early promise in some of the ideas for engineering proximity tracking apps, there are many open questions.

Would Proximity Apps Be Effective?

Traditional contact tracing is fairly labor intensive, but can be quite detailed. Public health workers interview the person with the disease to learn about their movements and people with whom they have been in close contact. This may include interviews with family members and others who may know more details. The public health work-

ers then contact these people to offer help and treatment as needed, and sometimes interview them to trace the chain of contacts further. It is difficult to do this at scale during a pandemic. In addition, human memory is fallible, so even the most detailed picture obtained through interviews may have significant gaps or mistakes.

Any proximity app contact tracing is not a substitute for public health workers' direct intervention. It is also doubtful that a proximity app could substantially help conduct COVID-19 contact tracing during a time like the present, when community transmission is so high that much of the general population is sheltering in place, and when there is not sufficient testing to track the virus. When there are so many undiagnosed infectious people in the population, a large portion of whom are asymptomatic, a proximity app will be unable to warn of most infection risks. Moreover, without rapid and widely available testing, even someone with symptoms cannot confirm to begin the notification process. And everyone is already being asked to avoid proximity to people outside their household.

However, such an app might be helpful with contact tracing when community transmission is low enough that the population can stop sheltering in place, and when there is sufficient testing to quickly and efficiently diagnose COVID-19 at scale.

Traditional contact tracing is only useful for contacts that the subject can identify. COVID-19 is exceptionally contagious and may be spread from person to person during even short encounters. A brief exchange between a grocery clerk and a customer, or between two passengers on public transportation, may be enough for one individual to infect the other. Most people don't collect contact information for everyone they encounter, but apps can do so automati-

cally. This might make them useful complements to traditional contact tracing.

But an app will treat the contact between two people passing on the sidewalk the same as the contact between roommates or romantic partners, though the latter carry much greater risks of transmission. Without testing an app in the real world—which entails privacy and security risks—we can't be sure that an app won't also log connections between people separated by walls or in two adjacent cars stopped at a light. Apps also don't take into account whether their users are wearing protective equipment, and may serially over-report exposure to users like hospital staff or grocery store workers, despite their extra precautions against infection. It is not clear how the technological constraints of Bluetooth proximity calculations will inform public health decisions to notify potentially infected individuals. Is it better for these applications to be slightly oversensitive and risk over-notifying individuals who may not have actually been standing within six feet of an infected user for the requisite amount of time? Or should the application have higher thresholds so that a notified user may have more confidence they were truly exposed?

Furthermore, these apps can only log contacts between two people who each have a phone on their person that is Bluetooth enabled and has the app installed. This highlights another necessary condition for a proximity app to be effective: its adoption by a sufficiently large number of people. The Apple and Google APIs attempt to address this problem by offering a common platform for health authorities and developers to build applications that offer common features and protections. These companies also aspire to build their own applications that will interoperate more directly and speed adoption.

But even then, a sizable percentage of the world's population—including a good part of the population of the United States—may not have access to a smartphone running the latest version of iOS or Android. This highlights the need to continue to employ tried-and-true public health measures such as testing and traditional contact tracing, to ensure that already-marginalized populations are not missed.

We cannot solve a pandemic by coding the perfect app. Hard societal problems are not solved by magical technology, among other reasons because not everyone will have access to the necessary smartphones and infrastructure to make this work.

Finally, we should not excessively rely on the promise of an unproven app to make critical decisions, like deciding who should stop sheltering in place and when. Reliable applications of this sort typically go through many rounds of development and layers of testing and quality assurance, all of which takes time. And even then, new apps often have bugs. A faulty proximity tracing app could lead to false positives, false negatives, or maybe both.

Would Proximity Apps Do Too Much Harm to Our Freedoms?

Any proximity app creates new risks for technology users. A log of a user's proximity to other users could be used to show who they associate with and infer what they were doing. Fear of disclosure of such proximity information might chill users from participating in expressive activity in public places. Vulnerable groups are often disparately burdened by surveillance technology, and proximity tracking may be no different. And proximity data or medical diagnoses might be stolen by adversaries like foreign governments or identity thieves.

To be sure, some commonly used technologies create similar risks. Many track and report your location, from Fitbit to Pokémon Go. Just carrying a mobile phone brings the risk of tracking through cell tower triangulation. Stores try to mine customer foot traffic through Bluetooth. Many users are "opted in" to services like Google's location services, which keep a detailed log of everywhere they have gone. Facebook attempts to quantify associations between people through myriad signals, including using face recognition to extract data from photographs, linking accounts to contact data, and mining digital interactions. Even privacy-preserving services like Signal can expose associations through metadata.

So the proposed addition of proximity tracking to these other extant forms of tracking would not be an entirely new threat vector. But the potentially global scale of contact tracing APIs and apps, and their collection of sensitive health and associational information, presents new risks for more users.

Context matters, of course. We face an unprecedented pandemic. Tens of thousands of people have died, and hundreds of millions of people have been instructed to shelter in place. A vaccine is expected to take 12 to 18 months. While this gives urgency to proximity app projects, we must also remember that this crisis will end, but new tracking technologies tend to stick around. Thus proximity app developers must be sure they are developing a technology that will preserve the privacy and liberty we all cherish, so we do not sacrifice fundamental rights in an emergency. Providing sufficient safeguards will help mitigate this risk. Full transparency about how the apps and the APIs operate, including open source code, is necessary

for people to understand, and give their informed consent to, the risks.

Does a Proximity App Have Sufficient Safeguards?

We urge app developers to provide, and users to require, the following necessary safeguards:

Consent

Informed, voluntary, and opt-in consent is the fundamental requirement for any application that tracks a user's interactions with others in the physical world. Moreover, people who choose to use the app and then learn they are ill must also have the choice of whether to share a log of their contacts. Governments must not require the use of any proximity application. Nor should there be informal pressure to use the app in exchange for access to government services. Similarly, private parties must not require the app's use in order to access physical spaces or obtain other benefits.

Individuals should also have the opportunity to turn off the proximity tracing app. Users who consent to some proximity tracking might not consent to other proximity tracking, for example, when they engage in particularly sensitive activities like visiting a medical provider, or engaging in political organizing. People can withhold this information from traditional contact tracing interviews with health workers, and digital contact tracing must not be more intrusive. People are more likely to turn on proximity apps in the first place (which may be good for public health) if they know they have the prerogative to turn it off and back on when they choose.

While it may be tempting to mandate use of a contact tracing app, the interference with personal autonomy is unacceptable. Public health requires trust between public health officials and the public, and fear of surveillance may cause individuals to avoid testing and treatment. This is a particularly acute concern in marginalized communities that have historical reasons to be wary of coerced participation in the name of public health. While some governments may disregard the consent of their citizens, we urge developers not to work with such governments.

Minimization

Any proximity tracking application for contact tracing should collect the least possible information. This is probably just a record of two users being near each other, measured through Bluetooth signal strength plus device types, and a unique, rotating marker for the other person's phone. The application should *not* collect location information. Nor should it collect time stamp information, except maybe the date (if public health officials think this is important to contact tracing).

The system should retain the information for the least possible amount of time, which likely is measured in days and weeks and not months. Public health officials should define the increment of time for which proximity data might be relevant to contact tracing. All data that is no longer relevant must be automatically deleted.

Any central authority that maintains or publishes databases of anonymous identifiers must not collect or store metadata (like IP addresses) that may link anonymous identifiers to real people.

The application should collect information *solely* for the purpose of contact tracing. Furthermore, there should be hard barriers between (a) the proximity tracking app and (b) anything else an app maker is collecting, such as aggregate location data or individual health records.

Finally, to the greatest extent possible, information collected should reside on a user's own device, rather than on servers run by the application developer or a public health entity. This presents engineering challenges. But lists of devices with which the user has been in proximity should stay on the user's own device, so that checking whether a user has encountered someone who is infected happens locally.

Information security

An application running in the background on a phone and logging a user's proximity to other users presents considerable information security risks. As always, limiting the attack surface and the amount of information collected will lower these risks. Developers should open-source their code and subject it to third-party audits and penetration testing. They should also publish details about their security practices.

Further engineering may be necessary to ensure that adversaries cannot compromise a proximity tracing system's effectiveness or derive revealing information about the users of the application. This would include preventing individuals from falsely reporting infections as a form of trolling or denial of service, as well ensuring that well-resourced adversaries who monitor metadata cannot identify individuals using the app or log their connections with others.

"Anonymous" identifiers must not be linkable. Regularly rotating identifiers used by the phone is a start, but if an adversary can learn that multiple identifiers belong to the same user, it greatly increases the risk that they can tie that activity to a real person. As we understand Apple and Google's proposal, users who test positive are asked to upload keys that tie together all their identifiers for a 24-hour period. (We have asked Apple and Google for clarification.) This could allow trackers to collect rotating identifiers if they had access to a widespread network of Bluetooth readers, then track the movements of infected users over time. This breaks the safeguards created by using rotating identifiers in the first place. For that reason, rotating identifiers must be uploaded to any central authority or database in a way that doesn't reveal the fact that many identifiers belong to the same person. This may require that the upload of a single user's tokens is batched with other user data or spread out over time.

Finally, governments might try to force tech developers to subvert the limits they set, such as changing the application to report contact lists to a central authority. Transparency will mitigate these risks, but they remain inherent in building and deploying such an application. This is one of the reasons we call on developers to draw clear lines about the uses of their products and to pledge to resist government efforts to meddle in the design, as we've seen companies like Apple do in the San Bernardino case.

Transparency

Entities that develop these apps must publish reports about what they are doing, how they are doing it, and why they are doing it. They

must also publish open source code, as well as policies that address the above privacy and information security issues. These should include commitments to avoid other uses of information collected by the app and a pledge to avoid government interference to the extent allowed by law. Stated as application policy, this should also allow enforcement of violations through consumer protection laws.

Addressing Bias

As discussed above, contact tracing applications will leave out individuals without access to the latest technology. They will also favor those predisposed to count on technology companies and the government to address their needs. We must ensure that developers and the government do not directly or indirectly leave out marginalized groups by relying on these applications to the exclusion of other interventions.

On the other side, these apps may lead to many more false positives for certain kinds of users, such as workers in the health or service sectors. This is another reason that contact-tracing apps must not be used as a basis to exclude people from work, public gatherings, or government benefits.

Expiration

When the COVID-19 crisis ends, any application built to fight the disease should end as well. Defining the end of the crisis will be a difficult question, so developers should ensure that users can opt out at any point. They should also consider building time limits into their applications themselves, along with regular check-ins with the users as to whether they want to continue broadcasting. Furthermore, as

major providers like Apple and Google throw their weight behind these applications, they should articulate the circumstances under which they will and will not build similar products in the future.

Technology has the power to amplify society's efforts to tackle complex problems, and this pandemic has already inspired many of the best and brightest. But we're also all too familiar with the ability of governments and private entities to deploy harmful tracking technologies. Above all, even as we fight COVID-19, we must ensure that the word "crisis" does not become a magic talisman that can be invoked to build new and ever more clever means of limiting people's freedoms through surveillance.

Face Surveillance and Thermal Imaging Cameras Are Not the Solution to the COVID-19 Crisis

As governments around the world continue to seek solutions to prevent the spread of COVID-19, companies are eager to sell their technology as a silver bullet to defeating the virus. And in the current moment, governments may be tempted to funnel scarce public health resources into the use of these technologies. Public health crises, especially a global pandemic, may require extraordinary measures in favor of the public good—but invasive face surveillance and thermal imaging cameras are not in the public's interest.

The Problems With Face Surveillance Haven't Gone Away

This approach could involve building new infrastructure to conduct more face surveillance and large government contracts with some of the most nefarious surveillance technology vendors in the world. Companies like Clearview AI, which uses over two billion face images scraped from social media to track individuals and identify them with real-time face surveillance, have been in talks with agencies to provide assistance. Even as civil liberties groups call for a national ban on government use of face recognition, U.S. Customs and Border Protection has touted face recognition at airport check-ins as supposedly more hygienic than other screening.

The massive infrastructure required to run face recognition (such as cameras, software, and open-ended contracts with vendors) cannot be easily dismantled when the public health crisis is over. We

cannot allow law enforcement and other government officials to normalize this invasive tactic. We know the truth about this spy tech: face recognition may seem convenient and useful, but is actually a deeply flawed technology that exposes people to constant scrutiny by the government, and has the potential to chill free speech and movement by identifying and tracking people as they visit their doctors, lawyers, houses of worship, or political demonstrations. It also can generate inaccurate reports.

It is all too likely that any new use of face surveillance to contain covid-19 would long outlive the public health emergency. In a year, systems that were put in place to track infected individuals as they moved through a city could be re-deployed to track people as they walk away from a political demonstration or their immigration attorney's office. Face recognition software that is able to identify people even when they're wearing surgical masks, as the company Hanwang has developed, could also be used to identify people who obscure their face at political protests out of fear of retribution from the government. We have to consider the afterlives of these technologies and the way their use can creep into everyday life after the emergency is over.

A Network Of Dubious Thermal Measuring Surveillance Cameras Are Still Surveillance Cameras

Some vendors of surveillance equipment advocate for the use of thermal cameras that would supposedly detect people who may be infected with the virus and walking around with a fever. These cameras threaten to build a future where public squares and sidewalks are

filled with constant video surveillance—and all for a technology that may not even be effective or accurate at detecting fevers or infection.

Thermal cameras are still surveillance cameras. Spending money to acquire and install infrastructure like so-called "fever detection" cameras increases the likelihood that the hardware will long outlive its usefulness during this public health crisis. Surveillance cameras in public places can chill free expression, movement, and association; aid in the targeted harassment and over-policing of vulnerable populations; and open the door to face recognition at a time when cities and states are attempting to ban it.

During a pandemic, it may be prudent to monitor a person's body temperature under specific circumstances. Hospitals are checking patient and staff temperatures at the door to make sure that no one with a fever unknowingly exposes the people inside the facility to the virus. In the San Francisco Bay Area, wearable rings are constantly monitoring the temperature of doctors and nurses treating COVID-19 patients to immediately alert them if they start to develop symptoms. This kind of tech can pose privacy risks depending on the privacy policy of the company that manufactures the rings, the hospital's own privacy policy, the data the technology collects, and who has access to that data. But these more focused programs are a far cry from dragnet surveillance cameras constantly surveilling the public—especially if those cameras don't function effectively.

Experts are now concluding that thermal imaging from a distance—including that in camera systems that claim to detect fevers—may not be effective. The cameras typically only have an accuracy of +/- 2 degrees Celsius (approximately +/- 4 degrees Fahrenheit) at best. This is cause for major concern. With such a wide range of vari-

ance, a camera might read a person's temperature as a very high 102.2 degrees Fahrenheit when they are actually running an average 98.5 degrees Fahrenheit. What's more, healthy human temperatures tend to vary widely, as much as 2 degrees Fahrenheit. Not only does this technology present privacy problems, but the problem of false positives cannot be ignored. False positives carry the very real risk of involuntary quarantine and/or harassment.

Thermal imaging seems even less likely to solve the COVID-19 pandemic given that a large number of people spreading the virus are doing so unknowingly because they are asymptomatic or have mild symptoms—mild enough to avoid triggering a "fever detecting" camera, even if it were running with perfect accuracy.

During this current moment, when governments are trying to hinder the spread of a contagion, technology companies are scrambling to prove that their goods are the solution we've been looking for. And while some of these companies may have tools that can help, a new network of surveillance cameras with dubious thermal measuring capabilities is not a tool we should deploy.

The Dangers of COVID-19 Surveillance Proposals to the Future of Protest

Many of the new surveillance powers now sought by the government to address the COVID-19 crisis would harm our First Amendment rights for years to come. People will be chilled and deterred from speaking out, protesting in public places, and associating with like-minded advocates if they fear scrutiny from cameras, drones, face recognition, thermal imaging, and location trackers. It is all too easy for governments to redeploy the infrastructure of surveillance from pandemic containment to political spying. It won't be easy to get the government to suspend its newly acquired tech and surveillance powers.

When this wave of the public health emergency is over and it becomes safe for most people to leave their homes, they may find a world with even more political debate than when they left it. A likely global recession, a new election season, and re-energized social movements will provide an overwhelming incentive for record numbers of people to speak out, to demonstrate in public places, and to demand concessions of their governments. The pent-up urge to take to the streets may bring mass protests like we have not seen in years. And what impact would new surveillance tools, adopted in the name of public health, have on this new era of marches, demonstrations, and strikes?

The collection and sharing of phone location data that was sold and deployed in order to trace the spread of the virus could be used by a reigning administration to crack down on dissent. The government and vendors have yet to make a convincing argument for how

this measure would contribute to the public health effort. Indeed, they cannot, because GPS data and cell site location information are not sufficiently granular to show whether two people were close enough together to transmit the virus (six feet). But this data is sufficiently precise to show whether a person attended a protest in a park, picketed in front of a factory, or traveled at night to the block where a dissident lives.

Many other technologies that should never be deployed to prevent the spread of the virus would also harm free speech. Vendors are seeking to sell face recognition cameras to the government to alert authorities if someone in mandatory quarantine went grocery shopping. They could just as easily be used to identify picketers opposing government initiatives or journalists meeting with confidential sources. For example, the infamous face surveillance company, Clearview AI, is in talks with the government to create a system that would use face recognition in public places to identify unknown people who may have been infected by a known carrier. This proposal would create a massive surveillance infrastructure, linked to billions of social media images, that could allow the government to readily identify people in public spaces, including protesters, by scanning footage of them against images found online. Likewise, thermal imagining cameras in public places will not be an effective means of finding people with a fever, given the high error rate when calculating a person's temperature at a distance. But police might be able to use such cameras to find protesters that have fled on foot from police engaged in excessive force against peaceful gatherings.

The U.S. government is not known for its inclination to give back surveillance powers seized during extraordinary moments.

Once used in acute circumstances, a tool stays in the toolbox until it is taken away. The government did not relinquish the power to tear gas protesters after the National Guard was called in to break up the Bonus Marchers assembled in the capitol during the Great Depression. Only after decades of clandestine use did the American people learn about the ways the FBI misused the threat of Communism to justify the wholesale harassment, surveillance, and sabotage of civil rights leaders and anti-war protesters. The revelation of these activities resulted in Sen. Frank Church's investigations into U.S. surveillance in the mid-1970s, the type of forceful oversight of intelligence agencies we need more of today. And the massive surveillance apparatus created by the PATRIOT Act after 9/11 remains mostly intact and operational even after revelations of its overreach, law-breaking, and large-scale data collection on U.S. persons.

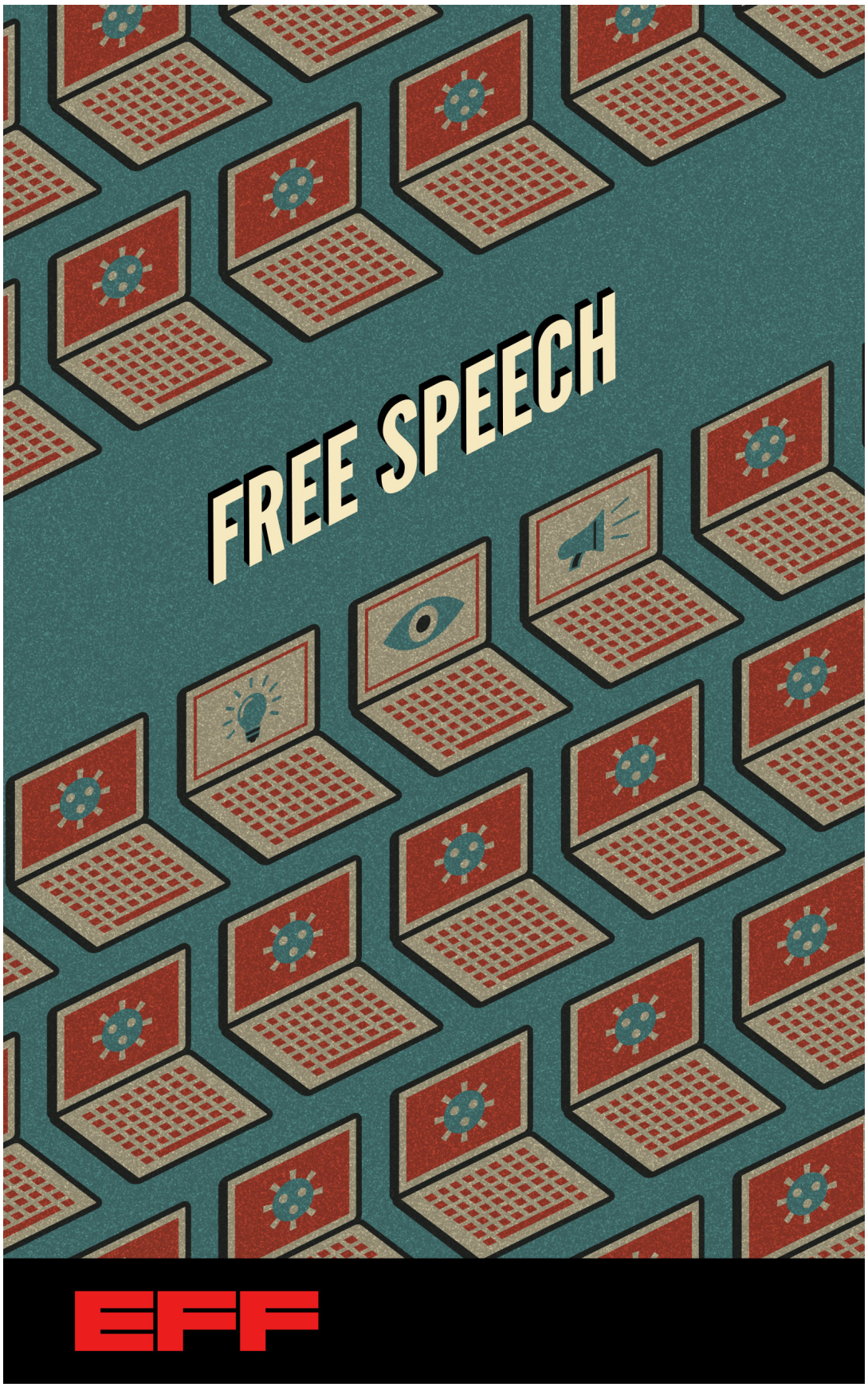
Even more proportionate technologies could be converted to less benign purposes than COVID-19 containment. Bluetooth-based proximity tracking apps are being used to trace the distance between two peoples' phones in an attempt to follow potential transmission of the virus. Done with privacy as a priority, these apps may be able to conceal the identities of people who come into contact with each other. Done wrong, these apps could be used to crack down on political expression. If police know that Alice was at a protest planning meeting, and police learn from the proximity app that Alice was near Bob that day, then police could infer that Bob was also at the meeting. Some versions of these apps also collect identifiers or geolocations, which could further be used to identify and track participants in protest planning meetings.

Done without collecting identifying information and minimizing storage, measures like aggregate geolocation tracking might assist public health response and be difficult to weaponize against protestors. But done with deliberate intention to survey demonstrations, aggregate location data might be disaggregated, merged with other data, and used to identify individual people. For example, police could single out individual protestors in a public plaza, track them to their respective homes and workplaces once the demonstration is over, and thereby identify them.

Free speech and political participation are chilled when governments put protests, protestors, activists, and organizers under surveillance. Studies have found that when people are aware of surveillance, they're less likely to engage in political speech or debate the important issues of the day. The First Amendment also protects the right of association for purposes of collective expression. This right is threatened if people are worried that they will be put under surveillance for joining or meeting with specific people or groups. Suddenly a person's movements, correspondence, or personal relationships are scrutinized by strangers within the government. At a moment when our society is desperate to find innovative solutions to daunting political problems, we should loudly condemn any surveillance efforts which might chill our ability to freely discuss and associate about pressing issues.

EFF has clear guidelines for how we evaluate whether a piece of surveillance technology, proposed as a tool of public health: Would it work? Is it too invasive? Are their sufficient safeguards? One of the biggest concerns is that new powers introduced at this current moment will long outstay their necessity, experience mission creep, and

by overtly redeployed for other purposes. Now, more than ever, we must stay vigilant about any new surveillance powers, technologies, and public-private relationships.


FREE SPEECH
EFF

SECTION 2: *Free Speech*

With the state of emergency, and the increased powers of government that comes with it, we must remain watchful for increased censorship. Indeed, the right of free expression is especially important when government is wielding such extraordinary powers, and the need for government oversight and accountability is great.

We remain vigilant in tracking, for example, anonymous whistle-blowing about containment efforts and online criticism of government responses to the crisis, and to the ability of prisoners to access social media to tell the world about the outbreak behind bars.

Social media plays an outsized role in many of our lives during normal times, and, for many, now even more so. As online platforms increase their reliance on automated content moderation—because human moderators cannot safely come to work—it is imperative that the expanded use of automation be temporary, transparent, and easily appealable.

The Right to Anonymity is Vital to Free Expression: Now and Always

As we're seeing many of our digital rights impacted by governments' handling of COVID-19, the right to anonymity remains vital. We've seen important medical information being shared with the press by anonymous health experts in Wuhan. We've also heard stories of vital information being suppressed, and arrests of those who speak out against their governments.

In times of turmoil, authorities might scapegoat anonymous speakers, blaming them for societal challenges. But anonymous speech is often how the public finds out the depth and severity of those challenges, be it an abuse of political power or the severity of a global pandemic. Without anonymous speech, some lies powerful people tell would go unchecked.

"*There are myriad reasons why individuals may wish to use a name other than the one they were born with. They may be concerned about threats to their lives or livelihoods, or they may risk political or economic retribution. They may wish to prevent discrimination or they may use a name that's easier to pronounce or spell in a given culture.*"

These words, from a blog post published nine years ago remain as true as ever. Whether we're talking about whistleblowers, victims of domestic violence, queer and trans youth who aren't out to their local communities, or human rights workers, secure anonymity is critical for these individuals, even life-saving.

And yet, our right to anonymity online remains at risk. Just in February 2020, British television presenter Caroline Flack's death by

suicide prompted calls for more regulation of social media, with some pundits suggesting platforms require ID. In India, a similar proposal is expected to be released by the country's IT Ministry, although reports indicate that verification would be optional.

Proponents of such proposals believe that when people use their "real" name, they behave more civilly toward one another. Facebook has long maintained that their policy requiring "authentic identity" keeps users safe. But the evidence just isn't there. One report, from the Coral Project, breaks down the fallacy of why people believe anonymity makes people less civil, while another—from commenting platform Disqus—suggests that people are at their kindest when using a pseudonym.

But most importantly, there are myriad reasons why anonymity and pseudonymity remain vital tools for free expression and safety. Take, for instance, our recent case involving Darkspilver, a member of the Jehovah's Witness community who posted comments—including a copy of an advertisement from the organization's Watchtower magazine—to Reddit. The Watchtower Bible and Tract Society pursued a copyright claim against Darkspilver over the advertisement. A magistrate judge ruled that the organization should be able to pursue its claim, and ordered the disclosure of Darkspilver's identity.

Darkspilver had serious concerns about being "disfellowshipped" from their community, having seen others cut off from their families and communities. EFF was able to successfully appeal in District Court, however, and Darkspilver's anonymity remains protected.

Automated Moderation Must be Temporary, Transparent and Easily Appealable

For many of us, social media has never been more crucial than it is right now: it's keeping us informed and connected during an unprecedented moment in time. People have been using major platforms for all kinds of things, from following and posting news, to organizing aid—such as coordinating the donations of masks across international boundaries—to learning yoga and gardening, sharing tips on working from home and, of course, for pure entertainment.

At the same time, the content moderation challenges faced by social media platforms have not disappeared—and in some cases have been exacerbated by the pandemic. In the past weeks, YouTube, Twitter, and Facebook have all made public statements about their moderation strategies at this time. While they differ in details, they all have one key element in common: the increased reliance on automated tools.

Setting aside the justifications for this decision—especially the concern that allowing content moderators to do that work from home may offer particular challenges to user privacy and moderator mental health—it will inevitably present problems for online expression. Automated technology doesn't work at scale; it can't read nuance in speech the way humans can, and for some languages it barely works at all. Over the years, we've seen the use of automation result in numerous wrongful takedowns. In short: automation is not a sufficient replacement for having a human in the loop.

It's important to give credit where credit is due. In their announcements, YouTube and Twitter both acknowledged the short-

comings of artificial intelligence, and are taking that into account as they moderate speech. YouTube will not be issuing strikes on video content except in cases where they have "high confidence" that it violates their rules, and Twitter will only be issuing temporary suspensions—not permanent bans—at this time. Facebook acknowledged that it will be relying on full-time employees to moderate certain types of content, such as terrorism.

These temporary measures will help mitigate the inevitable over-censorship that follows from the use of automated tools.

But history suggests that protocols adopted in times of crisis often persist when the crisis is over. Social media platforms should publicly commit, now, that they will restore and expand human review as soon as the crisis has abated. Until then, the meaningful transparency, notice, and robust appeals processes called for in the Santa Clara Principles will be more important than ever.

Notice and Appeals: We know the content moderation system is flawed, and that it's going to get worse before it gets better. So now more than ever, users need a way to get the mistakes fixed, quickly and fairly. That starts with clear and detailed notice of why content is taken down, combined with a simple, streamlined means of challenging and reversing improper takedown decisions.

Transparency: The most robust appeals process will do users little good if they don't know why their content is taken down. Moreover, without good data, users and researchers cannot review whether the takedowns were fair, unbiased, proportional, and respectful of users' rights, even subject to the exigencies of the crisis. That data should include how many posts were removed and ac-

counts permanently or temporarily suspended, for what reason, at whose behest.

The Santa Clara Principles provide a set of baseline standards to which all companies should adhere. But as companies turn to automation, they may not be enough. That's why, over the coming months, we will be engaging with civil society and the public in a series of consultations to expand and adapt these principles. Watch this space for more on that process.

Finally, platforms and policymakers operating in the EU should remember that using automation for content moderation may undermine user privacy. Often, automated decision-making will be based on the processing of users' personal data. As noted, however, automated content removal systems do not understand context, are notoriously inaccurate and prone to overblocking. The GDPR provides users, in its Article 22, with a right not to be subject to significant decisions that are based solely on automated processing of data. While this right is not absolute, it requires safeguarding user expectations and freedoms.

Now More Than Ever, Prisoners Should Have Access to Social Media

COVID-19 has trapped many of us in our homes, isolating us from family and friends and limiting our movements. But there are few people who feel the isolating impacts of COVID-19 more acutely than those who are *actually* incarcerated in jails and prisons across the country. As Jerry Metcalf, an inmate in Michigan, wrote for the Marshall Project's "Life on the Inside" series:

For those of you reading this who feel trapped or are going stir-crazy due to your coronavirus-induced confinement, the best advice I can give you—as someone used to suffering in long-term confinement—is to take a pause, inhale a few deep breaths, then look around at all the things you have to be grateful for.

Metcalf's is an important perspective to have, but, unfortunately, it is increasingly difficult to hear from inmates like him. That's because prison systems are making it harder for the public to hear from incarcerated people through excessive restrictions on the ways prisoners can express themselves over the Internet.

It's especially important to hear from Metcalf, and others like him, in this moment—given the heightened risk COVID-19 poses to inmates. The virus has already demonstrated an ability to move swiftly through closed spaces, like cruise ships and nursing homes—and it's already made its way into several prison systems, the consequences of which we'll sadly see unfold over the next several weeks. As Metcalf described it, COVID-19 has turned his prison into a "death trap." Given the potential humanitarian crisis many prisoners

now face, it's critically important to receive unvarnished reports from them about life inside prison walls.

For those outside of prison, social media has been an important tool during the pandemic—helping us connect with family and friends, to share updates and news, and to stay informed.

But, overwhelmingly, the incarcerated cannot connect to the outside world in this way.

We've long been concerned with government attempts to unduly limit prisoners' speech—especially by limiting access to technology that would allow the incarcerated to lift their voices beyond the prison walls. These restrictions come in a variety of forms, but one type we've paid particular attention to in the past is limitations on access to social media.

Many states prohibit inmates from accessing or posting information to social media in any manner. Some states, like Alabama and Iowa, go so far as to limit the ability of third-parties outside of prison—like a friend or relative—to post information to social media on an inmate's behalf. Some of these policies can even extend beyond what we typically think of as social media, prohibiting access to email or even *any* online publication of prisoners' speech (including, as a potential example, stories like Metcalf's published by the Marshall Project). Violations can carry extreme and disproportionate consequences. For example, some inmates in South Carolina received years in solitary confinement for posting on Facebook while in prison.

Even in calmer times, draconian limitations on social media access are dangerous and raise serious First Amendment concerns. Prisoners, and those who support them, use social media to raise

awareness about prison conditions; to garner support for court cases or clemency proceedings; and to otherwise advocate for important social and political issues.

As we've said before, invoking the immortal words of Martin Luther King, Jr, written from jail, which changed the course of civil rights in America: "Inmates may lose many liberties when they enter the correction system, but the ability to participate in debate online should not be one of them. Censorship of prisoners is also censorship of society at large because it deprives the public of the freedom to read the long letters, consider the long thoughts, and hear the long prayers of people who have lost their freedom."

The need to hear these voices now is particularly important—as prisons begin to close to outside visitors, and further isolate, in an attempt to stave off COVID-19. Jerry Metcalf's perspective—from inside a prison in Michigan in the midst of a global pandemic—is equally important if it's published by the Marshall Project or if it's shared by a relative in a Facebook post. What's important is that the world is able to hear his story, and those like him, right now.

As the pandemic unfolds, state agencies should take a flexible approach to enforcement of restrictions on inmates' ability to connect with the outside world, including curbing the enforcement of overly restrictive social media policies. We'll be carefully watching to make sure any restrictions that are applied are done so consistent with the First Amendment rights of inmates and those who support them.

Governments Need Critics—Especially During A Crisis

In late December, 2019, only a few hundred people knew of COVID-19. Now much of the world has had to learn about, adapt, and respond to the deadly disease. Though the highly contagious virus seems impossible to ignore today, it's in part thanks to whistleblowers and critics around the world sharing warnings and information that some governments responded to the pandemic when they did.

But even now, different governments are handling the crisis in a spectrum of ways: within the U.S., individual states have taken extraordinarily diverse approaches to controlling its spread, some nearly dismissing it, others implementing strict quarantine measures.

And rather than highlighting the need for increased transparency, some governments are using this as an opportunity to curb freedom of the press, limiting what can be reported, or putting out competing stories meant to shift the narrative away from the dangers of the disease or criticisms of their official response.

It's rarely been more important for individuals to be able to speak out and share information with one another online than in this moment. In a crisis—especially under authoritarian regimes, and in the absence of a trustworthy press—free expression is critical for people to engage with one another. Under governments that dismiss or distort scientific data, it may even be lifesaving.

Governments Misuse Crisis to Crack Down and Expand Laws

But as individuals comment on how officials are handling the situation—either to praise, critique, or ask questions—and people share potentially critical experiences and information with one another, some countries are using the opportunity to crack down dangerously on free speech.

Dr. Li Wenliang, the Chinese physician who warned colleagues of the deadly and contagious new virus in late December via a private WeChat message, has gained notoriety as a whistleblower. He was quickly accused by government officials of illegally posting rumors online when screenshots from his private messages were shared on public forums, which became the first place many heard of the virus. Li signed a police statement agreeing to cease spreading misinformation, and a few weeks later he passed away due to complications from having contracted coronavirus himself.

Li's warnings likely saved lives: his colleagues shared his message, which helped force officials into action. He has since been called a hero, and authorities have admitted to mishandling his case. But Li was not alone: seven other Chinese medical professionals blew the whistle about coronavirus early on.

Since then, hundreds more have been arrested by the "Internet police" in China for commenting about the situation online. Others have been arrested around the world for posting comments about the virus or for protesting government reactions to it. The governments of Cambodia, Malaysia, Palestine, Thailand, and Indonesia have all arrested individuals for spreading "misinformation." Many arrested were activists.

Singaporean officials are using the outbreak to justify legislation which gives new powers to limit "fake news" far beyond the scope of potential dangers to public health. In Morocco, individuals have been arrested for critiquing restrictions on public gatherings, and government officials have used this crisis to push forward new cybercrime laws limiting online speech. Egyptian police have arrested protestors for demanding the release of prisoners jailed dangerously close in overcrowded cells, including the family of free software developer and activist Alaa Abd El Fattah. And Egyptian officials have removed at least one journalist from the country for reporting on a study critical of the "official" number of cases.

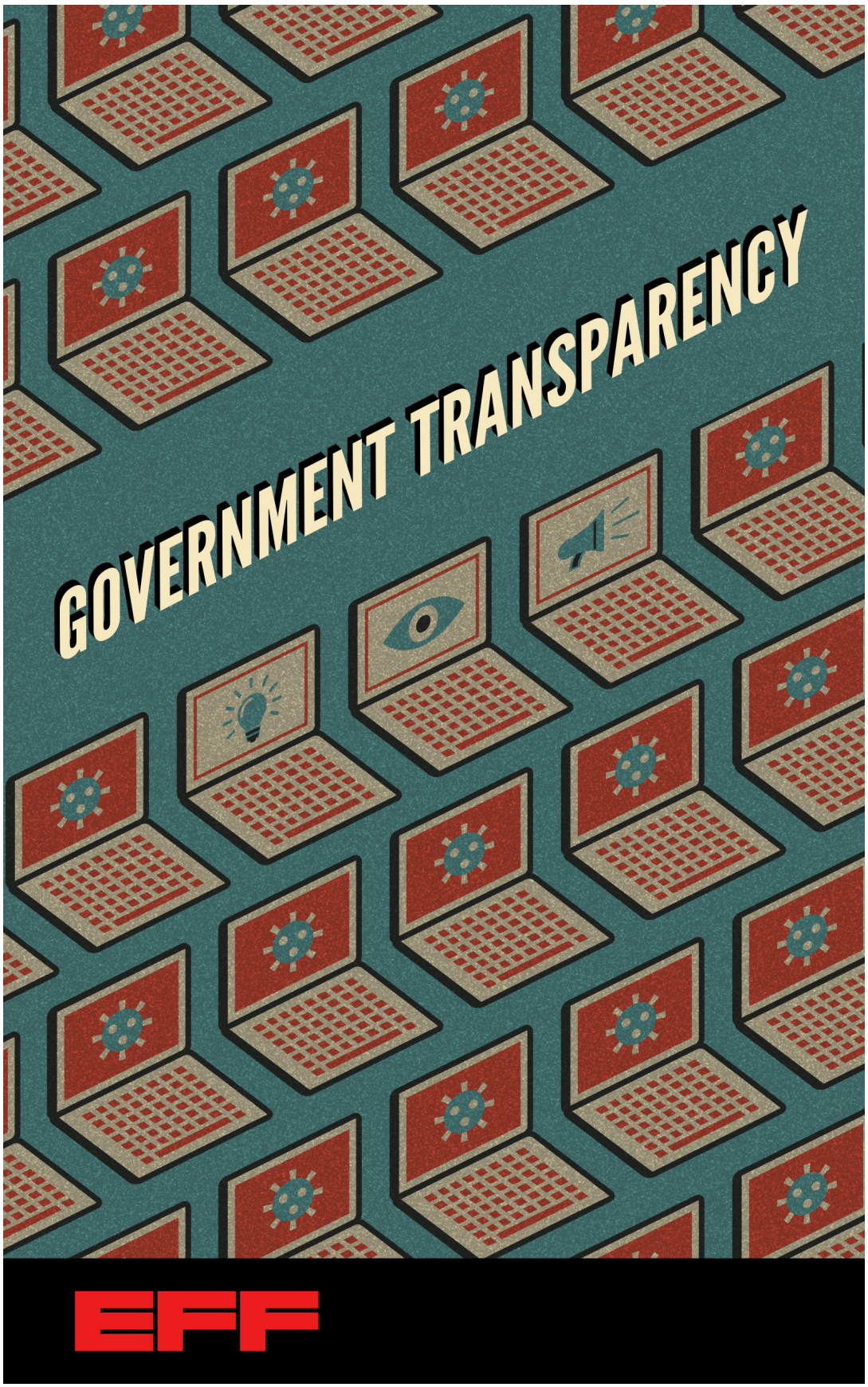
Healthy Societies Require More Than One Voice

Though some regimes are taking this moment as an opportunity to censor and even jail individuals for their opposition, it's heartening that there are also a number of stories of people coming together in innovative ways to aid one another, often in lieu of official government assistance. But in the rush to take in all the information available about the virus, often shared by individuals, not governments or the press, we can't lose sight of how countries may be building frameworks that cement in place what does or does not qualify as "information" or "misinformation." And while there's an important flurry of legislative activity to protect people affected by this crisis, it's important to remember that laws or regulations instituted now could be used to censor and overcorrect accurate, useful speech—sometimes the speech of those working together to help one another survive.

It's clearer when you look to Dr. Li. In this crisis, the stories of individuals coming together to aid one another often intersect with those being arrested or charged for protest or misinformation. Time has saved lives, helping us slow the spread of the disease through quarantines, testing, and simple public health notices about hand washing and keeping six feet apart from others. And throughout the crisis, it's frequently been those most at risk of retaliation—whistleblowers and government critics—who have given us that much-needed time by sounding the alarm.

Human rights workers, free expression advocates, bloggers, software developers, and activists are all in danger when government uses leeway obtained during a crisis to curtail free expression far beyond what's required. Governments must not take advantage of the COVID-19 pandemic to justify new limitations on speech. And they must not use this crisis as a tool to set in place new restrictions or regulations on whistleblowers, activists, or others who are sharing information.

"I think a healthy society should not have just one voice," Dr. Li told journalists just before his death, which sparked cries for an end to freedom of speech restrictions around the country. In this moment when the Internet has helped millions come together through quarantines and other difficult measures, laws restricting freedom of expression must not be expanded. Even dissenting voices are critical when the literal health of millions is at stake.


GOVERNMENT TRANSPARENCY
EFF

SECTION 3: *Government Transparency*

The right to access government policies, practices, and decision making is critically important as the public seeks to understand how the government is responding to the pandemic, and seeks to understand how the government is going about its other business during the pandemic. With the physical halls of government closed, governments must ensure that the public has access to both their records and proceedings. Legislative debate, court hearings, and other government proceedings that are required by law to be open to the public should be live-streamed or broadcast. And the government must continue to respond to public records requests and to make court records publicly available.

Governments Must Commit to Transparency During COVID-19 Crisis

As government officials at all levels move quickly to respond to COVID-19 and protect the public's health, it is vital that they also safeguard the public's ability to participate in and access information about those decisions, EFF and a coalition of more than 100 organizations wrote in an open letter.

Transparency and public access during this crisis are a necessary and important way to give those affected clarity into government decision-making. It's neither normal nor healthy for democracy to hide or classify public health-related decisions or deliberations. At a time when whistleblowers and others have contributed to the public awareness of how agencies and government actors, in the U.S. and abroad, have responded to this crisis, it's crucial that we see exactly how decisions with potentially life-altering ramifications are made. From the letter:

"At all times, but most especially during times of national crisis, trust and credibility are the government's most precious assets. As people are asked to make increasing sacrifices in their daily lives for the greater good of public health, the legitimacy of government decision-making requires a renewed commitment to transparency."

While some government functions move away from normal channels due to safety measures such as quarantines—for example, using video chat instead of in-person meetings—every effort must be made to ensure those channels allow for messages to be publicly accessible. Agencies may struggle to respond quickly to public records requests and other requests for information at this time, which is

why the default must be a commitment to transparency from the beginning, rather than obfuscation. For example, agencies should not follow the lead of the FBI, which stopped accepting FOIA requests via email.

The letter also encourages governments to postpone important decisions that can be made after the current crisis, as officials should not exploit the inability for the public to participate in person in the short term:

"Just as citizens are being asked to defer nonessential travel and errands, so should government agencies defer noncritical policy-making decisions until full and meaningful public involvement can be guaranteed. Where postponement is not realistic, every available measure should be taken to (1) notify the public of meetings of government bodies and how to participate in those meetings remotely, (2) use widely available technologies to maximize real-time public engagement, and (3) preserve a viewable record of proceedings that is promptly made accessible online."

Transparency is among the principles EFF has laid out for government to take into consideration and commit to during this crisis. Knowing "what the government is up to" is often the first step in ensuring that the government respects the civil liberties of its citizens, and during a crisis, this knowledge takes on extraordinary importance. Though this may take additional effort due to the severity of the pandemic, it is essential that government actions be clearly and quickly explained to the public. Moreover, transparency is particularly important so the public can scrutinize fast-moving efforts to have private companies work with the government to respond to

COVID-19, such as the reported Google effort to help broaden access to screening for the virus.

The rallying cry of these difficult times is that we're all in this together. We agree, and that includes keeping everyone in the loop when it comes to technology that could cause long-lasting damage to our rights after the crisis has passed.

The Time Is Now: The Supreme Court Must Allow Live Cameras

> *Subsequent to this article, The Supreme Court announced that it will broadcast live audio of their deliberations during the pandemic. This unprecedented decision is an important step forward for government transparency- though the public deserves live video as well.*

At a time when government officials are justifiably limiting in-person gatherings to slow the spread of COVID-19, the public should have access to essential government activities. The Supreme Court is no exception, which is why it must finally allow cameras in its courtroom.

Responding to the health and safety concerns raised by the spread of COVID-19, the Supreme Court announced on March 12 that it would close its building to the public until further notice. Four days later, the Court postponed its March oral arguments altogether.

Once the Supreme Court begins hearing oral arguments again, it must allow the public to access them by broadcasting or releasing same-day video recordings of its proceedings. Just as every other facet of life is moving to telecommunications platforms in response to COVID-19, if the Court remains shut to an in-person audience, it should make videos of its arguments available to the public instead.

The public's right to access court proceedings like oral arguments is one of the most basic tenets of our justice system, rooted in both the Constitution and common law. Access to courts safeguards

the foundation of our democracy by ensuring the public can see how courts operate, understand how they apply the law, and hold our justice system accountable so that the public's trust in it can be maintained. The Supreme Court recognized this principle more than 40 years ago, writing that "People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing."

In light of this longstanding mandate, Supreme Court arguments are open to the public and press. That means members of the public can travel to the Supreme Court building in Washington, D.C., to watch oral arguments in person (although courtroom capacity is limited). Additionally, the Court makes argument transcripts available day-of and releases audio at the end of the week.

Such access is important, but far from sufficient. The courtroom is fairly small, and those wishing to attend argument—even attorneys who are members of the Supreme Court bar—are typically required to line up early in the morning. Argument transcripts and audio recordings are not a perfect substitute for those who cannot travel to Washington D.C. or otherwise get into the courtroom. Non-verbal signals—an eye roll or disbelieving glare—can illuminate the justices' reasoning and provide valuable insight into the Court's ultimate decision.

While cameras are widely allowed in courtrooms at the trial and appellate levels, the Supreme Court has long resisted allowing cameras at argument.

This isn't because the Court hasn't considered it. Justice Kennedy has stated that videos in the Supreme Court are "inevitable." And in 1988, the Supreme Court secretly tested cameras in

the courtroom. Three Justices asked questions to Judge Timothy B. Dyk of the Court of Appeals for the Federal Circuit, who was, at that time, a media lawyer, and recorded the session to replicate a real oral argument.

But the Court didn't decide to allow cameras to access its courtroom then, and now, more than 30 years later, almost every Justice has publicly opposed doing so. Why?

Some Justices have expressed concern about how cameras would affect the lawyers arguing, perhaps by causing them to grandstand for the television.

But this hasn't proven to be the case in other courts that allow cameras. In a study by the Federal Judicial Center, judges and attorneys in such courtrooms agreed that cameras had little effect on trial participants. Canada's highest court has allowed cameras in the courtroom for over 30 years, and hasn't looked back. According to the former Canadian Chief Justice Beverly McLachlin, who served on the Canadian Supreme Court for over 28 years until retiring in 2017, the Canadian court originally had the same concerns about cameras—but it turns out that "nobody is out there trying to put on a performance." She said that she could only recall a single time where someone gave a "barnstorming kind of speech" in court that could have been directed at the cameras. And she "just told him to sit down."

Other Justices worry about the effect that cameras would have on them—perhaps by causing the Justices to self-censor at oral argument for fear that they might say something "ridiculous" or have their words taken out of context.

But any self-consciousness about the cameras likely wouldn't last long. Chief Justice McLachlin said that the Canadian Justices

there are “just oblivious" to the cameras. “I don’t think I ever think about them in the course of a hearing . . . They’re unobtrusive." And the Court already releases audio and written transcripts of arguments, so any gaffes are hardly a secret. To the extent that the Justices worry about their words being decontextualized or manipulated, the best remedy is to release accurate video in its entirety.

Even in normal times, when individuals can watch Supreme Court arguments in person, videos would allow the greater public to form opinions about the participants, the arguments presented, and the fairness of the procedures. Given the affordability and accessibility of video technology today, there is no justification for depriving the public of access to oral argument videos any longer.

Recognizing the public’s right of access includes the right to see what happens in the courtroom—on video if not in person—is all the more urgent with the Supreme Court now barring the press and public from attending in person.

EFF Joins Coalition Urging Judicial Transparency During the COVID-19 Emergency

EFF and a number of other organizations that advocate for government transparency signed onto a March 25 letter written by the First Amendment Coalition asking the California state judiciary to ensure public access to court proceedings and records during the COVID-19 crisis.

Many clerk's offices are restricting entry and many operations of the state court system have moved online in direct response to actions taken by Gov. Gavin Newsom, including the Statewide Order of March 23, 2020, which in effect restricted physical access to and the activities of California's courts. In the letter, addressed to Chief Justice Tani Cantil-Sakauye, coalition groups urge that while extraordinary measures are needed in the time of a public health emergency:

"we need to recognize that important civil liberties and constitutional rights should not be unduly restricted. While courts are closing buildings, halting proceedings and holding some hearings telephonically, we are concerned members of the press and public will face insurmountable barriers to access judicial records and proceedings."

Especially in times of crisis as governments make big decisions that could impact the safety and liberty of millions, it is more important than ever that government remain transparent and accessible when it comes to decision making. With so much to be decided, secrecy breeds distrust, panic, and conspiracy theories at a time when people need their government most.

To that end, the letter requests:

1. Telephonic hearings must be conducted on conference lines that make allowance for free public usage and dial-in information be made public ahead of the hearing.
2. Criminal proceedings must be conducted in a way that the public and press can still safely observe.
3. Court records must remain publicly available, and fees for online access waived, until normal operations resume.

These requests echo those EFF has made in other venues to preserve government transparency during the COVID-19 crisis.

For example, EFF also signed onto a letter urging local and state governments not to give into panic and secrecy by cutting people off from their right to know what the government is doing and what decisions they are making. "At all times," the letter said, "but most especially during times of national crisis, trust and credibility are the government's most precious assets. As people are asked to make increasing sacrifices in their daily lives for the greater good of public health, the legitimacy of government decision-making requires a renewed commitment to transparency." This included a rejection of the Federal Bureau of Investigation's decision to totally suspended accepting Freedom of Information Act requests.

EFF has also pushed for digital access to the arguments and processes of the U.S. Supreme Court as a way to make sure the American people are not shut off from the nation's highest court. Although the Court has suspended oral arguments, once it begins hearing them again, it must allow the public access by broadcasting or releasing same-day video recordings of its proceedings. The Supreme Court recognized the need for this transparency more than 40 years ago, writing that "People in an open society do not demand infallibility

from their institutions, but it is difficult for them to accept what they are prohibited from observing."

Whether it concerns actions dedicated to stop the spread of COVID-19, or just the general everyday operations of government, people have the right to know what their government is up to. In the era of social-distancing, this might require getting creative, but if we're all moving online to contend with the public health crisis, government transparency can too.

The California Public Records Act Is an Essential Right, Even During a State of Emergency

As Californians shelter-at-home up and down the state, the journalists and citizen watchdogs who file California Public Records Act (CPRA) requests know that trade-offs must be made. We know that local agencies may be understaffed at this time and that they may be slow to respond to our letters. They may need to restrict our ability to inspect records in person at City Hall, and public records lawsuits may stall as courts restrict hearing dates.

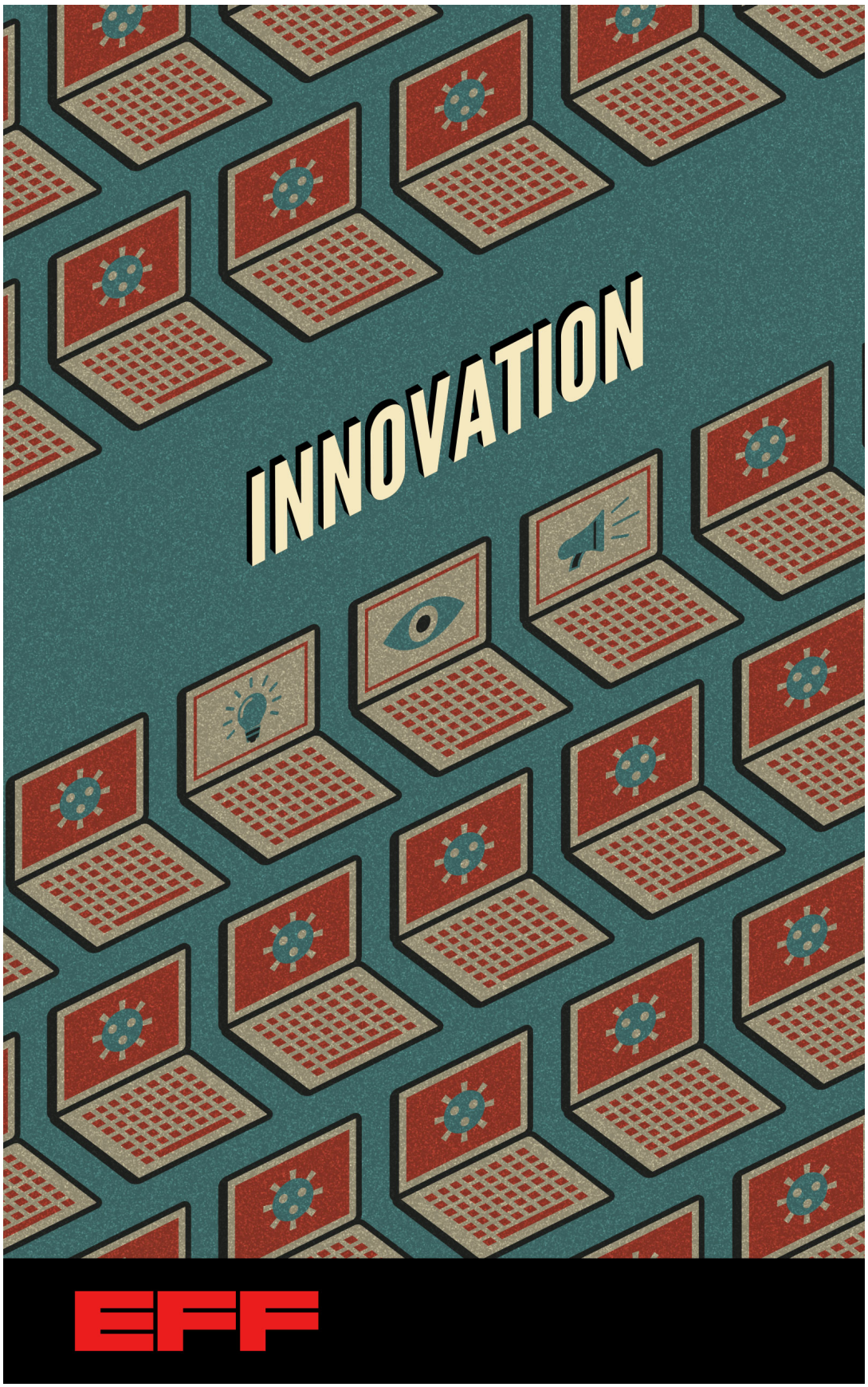
But where we draw the line is when government agencies announce they will suspend the public records request process altogether, a move telegraphed by several agencies in a recent Los Angeles Times story.

The right to access information is enshrined in the California Constitution, and this right is never more important than during an international crisis. That's why EFF has joined the First Amendment Coalition and other public records advocacy groups in signing a statement supporting government transparency, even amid the most challenging circumstances.

"While we acknowledge the extraordinary stresses that government agencies face right now, we urge all government agencies to comply with the California Public Records Act and the California Constitution and take all reasonable measures to continue to provide information to the public and the press during these exceptionally difficult times," the groups write.

The letter notes that COVID-19 is hardly California's first major crisis. The legislature has never authorized the suspension of CPRA, nor do Gov. Gavin Newsom's emergency orders waive agencies' responsibilities under CPRA.

The California Supreme Court has found that "openness in government is essential to the functioning of a democracy." While COVID-19 will certainly interrupt some of our normal expectations, it is essential that our democracy continue to function through these hard times. That means ensuring that the public can understand and hold officials accountable for the decisions they make in the halls of power while we're all stuck at home.


INNOVATION
EFF

SECTION 4: *Innovation*

A public health crisis on the scale of COVID-19 demands that researchers and innovators work together at scale to develop and implement solutions. Existing barriers to innovation and collaboration have become starkly visible during the pandemic, and removing those barriers has become more urgent than ever.

Academic publishers—infamously reticent as they often are to embrace open access—have taken unprecedented steps to make research that's useful in fighting COVID-19 available to a broad public. But at the same time, abuses of patent and copyright law threaten to undermine the public's ability to *use* the information contained in that research.

Patent abusers have taken advantage of the crisis, even reviving the patents from a long-defunct blood testing company in order to threaten companies offering COVID-19 tests today. And lobbyists for patent owners have even pushed members of Congress to *extend* patent terms for medical devices. The federal government should exercise its power to stop trolls from endangering COVID-19 testing and treatment. The COVID-19 crisis also demonstrates the ways in which manufacturers of medical devices can use copyright and other laws to unfairly restrict what owners can do with those devices, at a time when medical professionals are struggling to maintain and repair ventilators and other devices.

Right to Repair in Times of Pandemic

Entropy isn't just a word, it's the (second) law (of thermodynamics): the idea that things tend towards chaos and brokenness. That's why the Right to Repair is so close to our heart: fixing things is nothing less than the embodiment of the ancient struggle to wring order from chaos, to stave off deterioration and collapse.

It's no coincidence that farmers are the vanguard for Right to Repair. People who live in rural, low-population zones have to fend for themselves when entropy is visited upon their tools. Farmers can't wait for days or weeks for a part or a service technician: they literally have to make hay while the sun shines. Since the dawn of agriculture, farmers have been making and adapting their tools, and workshops and even forges are mainstays of agricultural life.

Coronavirus has given us all a taste of what life is like for farmers and other people far from repair and parts. With global supply chains in chaos and whole cities on lockdown, broken things might not get fixed unless you can fix them.

Lucky for us, we still have the Internet, which is full of repair instructions (including iFixit's massive repository of "repair guides for every thing") and we have more access to tools than at any time in history, including—for some of us—futuristic tools-that-make-tools, like laser-cutters, CNC mills, and 3D printers.

These have already begun to play a key role in the pandemic. A hospital in Brescia, Italy reportedly rehabilitated a broken, urgently needed Venturi oxygen mask for the hospital's ventilator with help from local 3D printing entrepreneurs who brought their printer to the hospital, designed a replacement part on the spot, and printed it

out, successfully repairing the respirator so that it could be used to save lives.

The story is a heartwarming mix of modern miracle and solidarity in a crisis, but there's more going on under the surface.

It turns out that the reason that the part had to be designed from scratch is that the manufacturer refused to help with the project. One of the people involved says that he was threatened with patent litigation if he tried; his colleagues differ on the matter, but they agree that the company refused to share design files. And sending threats or not, the part's designer still says he will not distribute the plans for a replacement.

All around the world, there is a shortage of ventilators and ventilator parts—and at the same time, the country that does the lion's share of high-tech manufacturing, China, is running at extremely reduced capacity. While online communities are crowdsourcing multiple plans for open source hardware ventilators and other pandemic-related technology, the most important thing they and companies can do is work in concert to keep existing, tested tech functional.

Getting this kind of med-tech project right is important, and it's hard. The global supply-chain shutdown has revealed the fragility of long distance, complex manufacturing systems that are organized around central hubs that represent points of critical failure. The surge in open source hardware designs and parts for medical equipment during the emergency represents a distributed, urgently needed decentralization of our world's critical manufacturing capacity. Even as these distributed efforts reduce the hazards of failing health systems, they have the potential to create their own hazards. The best way to ensure that emergency repairs and modifications are

safe is for original manufacturers to cooperate with community technicians. Indeed, that's the only way—we can't simply leave our hospitals undersupplied or sitting on broken hardware until the emergency has passed.

The very nature of emergency medicine means that front-line professionals must make decisions about how to keep their equipment running when it is not fully functional. Even under normal circumstances, there aren't always timely, reliable sources of parts and skilled service. The right person to decide whether a field repair should be attempted, and whether the repair is solid enough to rely upon are medical professionals, not the shareholders of med-tech companies or the lawyers who write their terms of service and patent applications.

We are all like farmers now—isolated, with machinery that we can't afford to let sit idle until a distant company can help us repair it. Today, we need those companies to step up by providing repair instructions, specifications, and technical aid to the global volunteer corps of makers and fixers who have given themselves over to helping us all weather this calamity.

Embracing Open Science in a Medical Crisis

Responding to the threat of COVID-19, science advisers from twelve countries signed on to an open letter urging scientific publishers to make all COVID-19 research freely available to the public through PubMed Central or the World Health Organization's COVID Database.

This is an emergency call for open science, the movement to make tools, data, and publications resulting from publicly funded research available to the public. Among the signers of this open letter was the Director of the United States Office of Science and Technology Policy, Kelvin Droegemeier, who is reportedly shaping an executive order to require similar availability for all federally funded research starting on the first day of publication.

Thankfully, major commercial publishers such as Elsevier and Springer have already announced that they will drop their paywalls on coronavirus research for the duration of the crisis. In doing so, a growing number of publishers are helping scientists work together to combat COVID-19 by embracing open access, the idea that research publications should be freely available for anyone to read.

That's a great start. Open access ensures scientists are operating transparently and have access to the most current information available. This allows research efforts to move more quickly and eliminates barriers among researchers across the globe. The current crisis demonstrates how open access is a human rights issue. Potentially life-saving medical knowledge should not be restricted to those connected to institutions that can afford expensive journal subscriptions.

Researchers have embraced libre and open source research tools such as Nextstrain and open data platforms like Gisaid. The combined efforts of scientific researchers and free software programmers have accelerated research on coronavirus to unprecedented speeds. Medical professionals are even working together to share information about how to repair vital equipment while others build open hardware alternatives to proprietary devices. Readers should keep in mind when interpreting the findings of these efforts, that they can often be shared before undergoing peer-review.

In the past decade we've come a long way in bringing scientific research to the public, but we're still far from realizing its full potential. Between a 2013 executive order and a 2018 California law, publishers are generally only required to make research freely available after a one-year embargo, and even then only if they receive federal or California state funding. While both are steps in the right direction, the current moment highlights why we need to go further. For fast-moving health research, a one-year embargo period severely reduces the value of an open access law for the public. A growing list of foundations have made that point clearly by requiring the research they fund to be open access on the day it's published.

In Europe, today's emergency support of open science is poised to become the status quo next year when the Plan S policy will require open access on the first day of publication. This means researchers will be in a better position to respond to future crises, and even more important discoveries will be made available through open access.

Researchers and publishers have made heroic strides this month, and we cannot forget the impact we are seeing in improving

public access to knowledge. It will become increasingly important to push for the full benefit of research by changing more state and federal laws to make open science the default, and go beyond reading access to grant greater re-use freedoms. Let's work together to help make the public better prepared for future crises.

Open Innovation in Medical Technology Will Save Lives

Experts from the world's top engineering programs have come together to share knowledge about medical technology, hoping to make life-saving treatments more widely available. Importantly, they're ensuring that patents, copyrights, and other legal restrictions don't get between that knowledge and the people who need it most.

Open Licenses Provide Life-Saving Technology in a Crisis

The availability of ventilators has emerged as a limiting factor in treatment of the COVID-19 virus, prompting researchers to imagine alternatives to the proprietary machines most commonly in use, which cost $30,000 each. At the forefront of this wave of innovation are experts at universities like MIT and Rice, demonstrating that open innovation isn't just the realm of do-it-yourself hobbyists, but the world's top engineering and medical minds.

Engineering teams are working on ways to adapt existing, medical-grade supplies that hospitals already have on hand to act as an emergency substitute for ventilators when better machines are not available. (Other low-cost ventilator units have been developed by teams such as one at Stanford, but would require the better part of a year to ramp up manufacturing.)

When a crisis highlights the flaws in the status quo, responsible innovators can provide a path forward and save lives. A read through the MIT project's resource page illustrates the complexity and perils of this project: the device must be both safe and useful, it must not

provide a false sense of efficacy that delays a patient's transfer to a different means of treatment, and it must measure and present certain data to enable doctors to monitor their patients' conditions. In addition to publishing their designs, the team is publishing the requirements that clinicians have communicated to them and the results of testing the device. In a short time, the team has already published data on the use of these devices in pigs.

All of this collaboration is enabled by open licensing such as Creative Commons and free or "libre" software licenses, which provide for the easy sharing and modification of the source material. And working in the open doesn't mean a sacrifice in quality. Rather, scientists know that the best way to understand a problem and create innovative solutions is through open collaboration. No one should have the veto power of copyright or patent law to prevent the sharing of knowledge about how to combat disease or build a life-saving device. Decisions about how to adjust medical devices in the field should be made by engineering and medical professionals, not the attorney who filed for a patent on it.

Some Companies are Promising Not to Enforce Their IP Rights

Old patents and copyrights that have nothing to do with COVID-19 can still get in the way of COVID-19 research taking place today. We've written about Labrador Diagnostics, the patent troll that sued a company for offering COVID-19 tests. Labrador's portfolio of patents came from Theranos, the fraudulent blood testing company that closed in 2018. Even though Labrador didn't have a working product—and Theranos' technology underlying its patents was dubi-

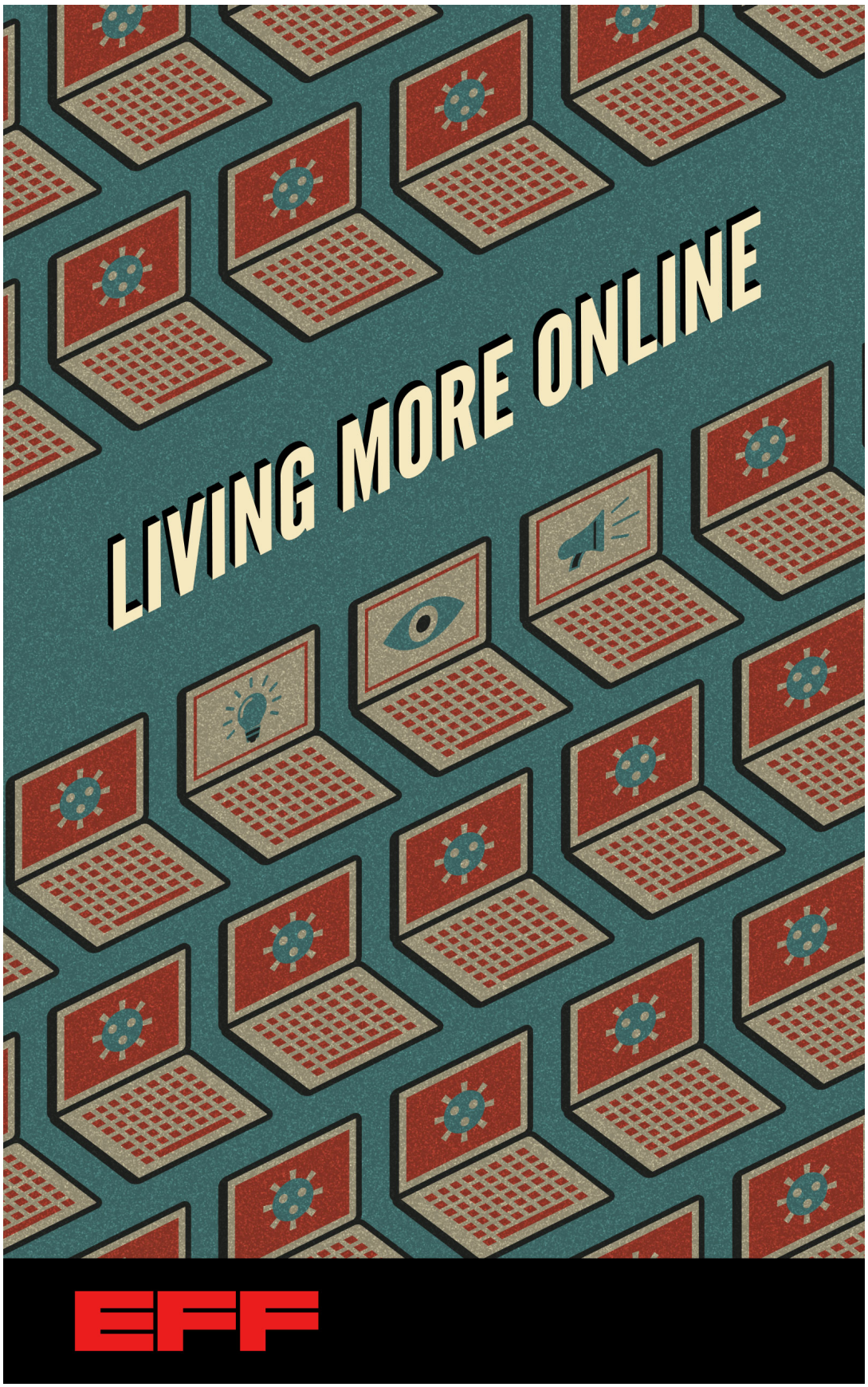
ous, to say the least—those patents still got in the way of lifesaving work. That's why it's essential that governments limit the damage that patent abusers can do to the fight against COVID-19. In recent weeks, lawmakers in Canada, Chile, Ecuador, Germany, and Israel have taken steps to disentangle COVID-19 research from patent abuse through compulsory licenses.

Some companies have done their part to ensure that their intellectual property holdings don't get in the way of the fight against COVID-19 either. The Open COVID Pledge is a simple pledge an IP owner can take not to assert its patents or copyrights against a company or organization fighting COVID-19. Tech giant Intel and Unified Patents were the first two companies to sign the pledge. While the Open COVID Pledge is certainly a much narrower commitment than persistent open licenses, it does ensure that those companies won't stand in the way of the fight against this pandemic.

Lobbyists for patent owners have pushed a narrative that current laws are insufficiently protective of patents to fight COVID-19, even arguing for a bill that would add an extra ten years to the patent term for pharmaceuticals and medical devices. It's absurd to think that the medical experts leading the fight against the virus are holding back their creativity until they get additional patent protections. This proposal also ignores the reality that the public is already paying for a substantial portion of medical research in the United States—including research into affordable ventilators. It's in the public's best interest to have those technologies shared far and wide, not encumbered by patent and copyright restrictions.

The false premise underlying proposals like these is that innovation depends on the financial incentive provided by monopolies.

Open innovation belies the idea that monopoly-based markets guide the best research decisions. Of course, research requires resources and skilled scientists. But a monopoly on the insights and innovations that research produces is far from the only way or the best way to encourage work that will improve—and even save—lives.


LIVING MORE ONLINE
EFF

SECTION 5: *Living More Online*

Social distancing is causing many of us to spend more time on the Internet. That dependence is only going to grow as time goes on. As parents depend on the Internet for distance learning, as businesses depend on employees being able to work from home, and as everyone depends on the Internet for public safety information, this pandemic has shone a spotlight on the ways that our current Internet ecosystem is failing many Americans, and made it abundantly clear that policymakers and ISPs must redouble efforts to build fiber for all, so that all Americans have fast and competitively-priced Internet access.

Bringing accessible, high-speed Internet to everyone in the country is only a start. As we rely on more online tools to make working from home and distance learning possible, Internet users should update their surveillance self-defense knowledge, for example, to make informed decisions about using online meeting tools and organizing online mutual aid efforts. Even during this public health crisis, you can protect the security and privacy of your daily life, so we've compiled guides to help users make informed decisions about what works best for you and your communities.

And lastly, as people rely more heavily on the Internet to form and maintain community, and to stand in for their schools, museums, and libraries, they are also finding themselves on the pointy end of a number of legal swords, particularly with regard to copyright. But this is a moment to strengthen fair use, the doctrine that safeguards creativity and free speech in a world where copyright gives exclusive control of some kinds of expression to the copyright holder. COVID-19 has created, almost by definition, a new and powerful public interest

purpose that must be considered in any fair use analysis. We applaud everyone rallying in favor of sharing our common culture, like the universities, private companies, and nonprofits making their intellectual property available free of charge. As always, fair use has a posse at EFF.

Social Distancing, The Digital Divide, and Fixing This Going Forward

Social distancing, work from home, shelter in place—these are all strategies employed in response to the COVID-19 epidemic. Americans who have jobs allowing them to engage in social distancing are very dependent on their Internet connection. That dependence is only going to grow as time goes on. As parents depend on the Internet for homeschooling, as businesses depend on employees being able to work from home, and as everyone depends on the Internet for public safety information, we need to recognize that our current Internet ecosystem is failing many Americans. And any infrastructure recovery effort that comes out of this situation should address the digital divide at its source: policy decisions that have left us at the mercy of a few, giant companies whose business concerns don't include *all* Americans.

For however long this emergency lasts, an untold number of us will be forced to deal with the failure of our telecom policies to produce universally available, affordable, and competitive high-speed broadband options. Families with children who must simultaneously handle school closures and remote education while also working through video conferencing and cloud computing will reside in the two different Americas for broadband access. American households who reap the benefits of competition among ever increasing speeds with lowering prices and Americans who are forced to rely on obsolete infrastructure built from a bygone era or, worse yet, have no broadband options at all. Those two Americas still being split between what we call the "digital divide" in 2020 is a clear sign of failure in our cur-

rent approach to broadband. It is imperative that we take it upon ourselves to forcefully bring an end to the inequality of access as part of any infrastructure recovery effort.

We Are Seeing the Digital Divide at Work, and Its Lines Are Drawn Where Fiber Access Exists

It could not be more clear: where there are upgraded networks—meaning networks that can deliver gigabit connections—those homes are able to handle the increase in Internet usage that social distancing requires. Where those networks do not exist—where Americans do not have choices for high-capacity services—social distancing is much harder on people, if not outright impossible.

Upgraded networks generally have had fiber infrastructure built by new, local, independent ISPs from both private and public providers. This new competition forced the old ISPs—often the usual suspects of AT&T, Verizon, and so on—to improve their own networks to keep pace. Not only did competition improve the *quality* of Internet service, it also improved the *price*.

But there are many Americans who don't have meaningful access to choice for high-speed broadband. Some have no choice at all. Communities that rely on decades-old Internet infrastructure lack access to an Internet connection that can handle the demands of social distancing. And the fault of this will lie with the ISPs who used record profits and tax cuts on everything but upgrading their services. The fault will also lie with our federal and state governments, which failed to promote fiber through laws pushing universality or funding to simply have someone besides the large incumbents build it.

Those relying on older networks are those who can least afford to: low-income and/or rural Americans. The most expensive part of starting an ISP is the initial construction cost. The legacy ISPs serving low-income and/or rural populations with older infrastructure have long since paid off that cost, but they still charge through the nose because their customers don't have alternative choices. And the number one reason people do not subscribe to broadband at all is excessive price. Because no one is offering better service, at a better price, there is no reason for these companies to upgrade their networks, leaving many Americans without the high-speed, reliable, competitively priced Internet service that we absolutely need, especially now.

The differences between competitive markets in the United States and noncompetitive ones is stark. Aside from higher prices and inferior infrastructure, even the COVID-19 oriented relief packages are dramatically different. For example, AT&T is waiving overage fees (a fraction of the excessive bill most people pay) and Comcast is offering 25 mbps/3 Mbps for free for two months to low-income users, but a fiber competitor called Sonic in San Francisco (a city with a fairly decent amount of competition) is offering free gigabit service for three months to families and seniors regardless of their income status.

High-Speed Affordable Broadband Is Essential for Everyone—and That Makes It a Sound Investment

What is tragic about the digital divide is that there are no good reasons for it to exist, let alone continue. It is profitable to serve *all* Americans, no matter what major incumbents like AT&T and Verizon may say. If the major ISPs universally converted their older networks

over to fiber to the home, they would be net profitable in the long run. Contrary to assertions that smartphones and wireless plans alone are sufficient, nothing can truly substitute for a high-capacity connection in the home. As we are seeing right now, the more and more we do online, the less and less our phones and our outside-the-home options will be compelling replacements.

Our own analysis of the world's fastest ISP demonstrates how the financials work for fiber networks. That ISP is located in the United States, built and run by the local government of Chattanooga, Tennessee. Once a portion of their network had subscribers, their revenue from $70 a month for gigabit service outpaced their costs for the entire network. In other words, after they reached a certain number of customers, their profits grew faster than their costs. That profit allowed them to stretch the network further and further. In fact, because of the unique nature of fiber wires, they were able to upgrade to a 10-gigabit network with only a tiny additional investment. Unfortunately—and predictably—the old ISPs stepped in and got states to ban local government broadband, crushing further expansion by this successful competitor. Extending fiber networks is perfectly doable, blocked only by the refusal of the big ISPs to do it themselves and their successful campaign to erect legal barriers to stymie alternatives.

But even that hasn't worked entirely. Because we need the Internet. And in a reversal of the classic movie quote, we're already there, so we will build it. In the state of Utah, where residents had been left behind by incumbent ISPs, and where the state law banning community broadband remains, a handful of cities collectively started building universal open access fiber as a workaround. To butcher another movie quote, we will not be ignored.

Rather than build broadband, they built fiber infrastructure, and allowed small private broadband companies to sell services off the network. Demand is so high for the services from these neglected communities, that more than enough money is being made. In fact, they've made enough to pay for the entire construction effort. This is allowing the network (called Utopia Fiber) to rapidly expand and complete universal fiber deployments on schedule, all while giving people nearly a dozen broadband options at competitive prices.

In response to COVID-19, they are currently experiencing a record number of new subscriptions from the people of Utah who need more capacity to stay home for long periods of time. Everywhere in the country we continue to see pockets of success, from the 7,000-member People's Rural Telephone Cooperative in Kentucky to nearly 100+ other small rural cooperatives deploying fiber to the home.

All of this shows not only that building fiber networks could have been done everywhere, for everyone, years ago, but also that it would have been profitable. So why have our big ISPs failed us?

The answer lies in their investor expectations and the companies' lack of willingness to engage in long-term investments versus faster short-term profits. Fiber networks are big investments that generally need 10 years or more to fully pay down the construction costs. Similar to when you buy a car, it comes with a big down payment, but eventually you have paid it off and just have maintenance costs. The difference here is that unlike your car, which depreciates after you buy it with higher maintenance costs over time, a fiber network will grow in value and usefulness because advancements in technology will allow it to get faster without any new down payments for construction. It is also expected to be useful for around 70 years after it is

built. It's a future-proof investment—the old ISPs just lack an interest in the future.

Since the old ISPs have proven unwilling to invest in what we need, no relief package or infrastructure package should defer to them on what to do. We should conclude that, after billions in tax breaks and federal deregulation by the FCC, that they are content with leaving people using decades-old infrastructure forever. After all, it is not like companies like AT&T are afraid of spending money when it comes to buying other companies, as their merger debt is an eye popping $171 billion (which is less than it would cost to give every single American a fiber connection).

Ending the Digital Divide Depends on Federal and State Infrastructure Plans That Deliver High-Speed Internet to Everyone

The unnecessary hardships many Americans face to maintain their daily lives are the inevitable result of relentlessly low expectations pushed by the big, old ISPs. They've set the bar so low in hopes that the public and the government would just accept a fraction of what Americans deserve from the broadband carrier industry. This has resulted in too many policymakers engaging in rhetoric about the importance of broadband, rather than putting forth policies that would give every American affordable 21st century-ready Internet access as a matter of law. It is time for policymakers to back up their rhetoric with action.

EFF supports universal deployment of fiber optics and open access policies that would promote competition and affordability not as

a pipe dream, but because we've seen the proof. Other countries are further along, giving us proof of concept.

So here's what we know: we need to be willing to invest, both with dollars and with our laws, in the goal of connecting everyone by a specific date. We need to also refocus our laws in remedying the lack of competition in the broadband access market. Our own engineering analysis shows that a broadband access network that is all fiber will be more than ready for advances in applications and services for decades to come, including massive increases in usage needs. Countries like South Korea that long ago completed their universal fiber build did so because the government's telecom policy drove that result.

As we noted in comments to the federal government and in our home state of California, the absence of a policy effort from government to push for guaranteed universality of fiber will continue the digital divide problem and worse yet replace it with a "speed chasm" of broadband choices. That means allowing the current state of affairs in the United States to continue is a choice. Let the hard lessons we are learning in real time today be the reason we finally commit to getting everyone connected in the aftermath.

The absence of universal access to high-speed, affordable Internet has made social distancing, working from home, remote education for children, and connecting with loved ones unnecessarily difficult. As Congress, the state governments, and local governments work to provide relief to Americans and the economy, any Internet infrastructure spending needs to remember this lesson.

Sharing Our Common Culture in Uncommon Times

We are in an unprecedented time. People are being told to stay home as much as possible. Some of us are lucky enough to have jobs that can be done remotely, schools are closed and kids are home, and healthcare, grocery, or other essential workers are looking for respite where they can safely find it. All of which means that, for now, for many of us, the Internet is not only our town square, but also our school, art gallery, museum, and library.

Users around the U.S.—from individual creators to libraries to educators to community organizers—are rising to the challenge this presents by going online to share information, music, books, and art. High-profile examples include LeVar Burton telling stories to children and adults alike and the cast of Hamilton reuniting via a YouTube show. Musicians of all levels of fame are performing through a wide range of services and apps. Teachers are taking on the tremendous task of educating online, rapidly finding, developing and sharing resources so that their students don't have to lose their place while they shelter in place. In response to the temporary closure of libraries around the US and abroad, the Internet Archive has created a National Emergency Library (NEL) that gives members of the public digital access to 1.5 million books, without charge. Universities, private companies, and nonprofits are pledging to make their intellectual property available free of charge as needed to fight the COVID pandemic and minimize its impacts.

But with more and more people relying on the Internet to form and maintain community, more and more people are also finding

themselves on the pointy end of a number of legal swords. Copyright, in particular, has become a potential threat. For example, celebrity doctor Dr. Drew tried to use bogus copyright claims to shut down a video compilation of his incorrect advice about the coronavirus. Burton said copyright worries had limited his reading choices. Others are getting caught in automated filtering machines, like the man who used Facebook Live to stream video of himself playing the violin, or the teacher trying to do a webcast for her Pre-K class while her husband was watching WrestleMania in the background. The Author's Guild and others are up in arms about the NEL, insisting it will destroy authors' livelihoods.

Those challenges are predictable, but it's heartening to see so many rallying in favor of sharing our common culture. When LeVar Burton expressed concern about copyright liability, authors such as Neil Gaiman and our own Cory Doctorow stepped up to grant permission. The International Federation of Library Associations has drafted an open letter to the World Intellectual Property Organization calling on WIPO and its members to do their part to facilitate public interest uses of work, and for rightsholders to do the same, and more than 312 organizations have signed on in less than a week.

As for the NEL, the New Yorker called it a "gift to readers," and more than 300 individuals and institutions have endorsed the project. The Internet Archive has put out a detailed response to its critics, explaining how the project works, why it is legally protected, and how authors can opt out if they wish. It's important to emphasize that the NEL only lends books for two weeks, after which the copy automatically disappears off of the user's device. Moreover, the NEL does not offer new releases, as the collection excludes titles published within the last five years, and authors or publishers can request that a title be

removed. And as Jonathan Band notes, there is no mechanism for the Internet Archive, or any other library, to license emergency access to many of the books in the collection. Finally, while the Archive does not closely log reader habits—showing a laudable and necessary respect for reader privacy – the information the Archive can share suggests that the NEL is not significantly affecting ebook licensing. Most books are only "opened" for less than 30 minutes, which suggests readers are using the NEL to browse and/or they are not interested in the PDF copy the Archive lends, which is significantly less reader-friendly than what you might see on your Kindle. The Archive also notes that 90% of the books that are borrowed were published a decade or more ago.

Fair Use Has a Posse

Many of these disputes over sharing culture are being played out in the court of public opinion for now, but users should know that there are strong legal protections as well. For example, our friends at American University have put together an outstanding primer for teachers on copyright and online learning. As they explain, the fair use doctrine protects many online learning practices, including reading aloud. Library adviser Kyle Courtney also has a great explainer on libraries, fair use, and exigent circumstances.

In a nutshell, the fair use doctrine allows you to use a copyrighted work without permission in a variety of circumstances. It is how we safeguard creativity and free speech in a world where copyright gives exclusive control of some kinds of expression to the copyright holder. To decide where a use is fair, courts consider the second user's *purpose* (Is it new and different from that of the original creator? Is it commercial or for-profit?); the *nature* of the original work (Was it

factual or fictional? Published or unpublished?); *how much* of the original work was used (Was it more than necessary to accomplish the second user's purpose?); and *market harm* (Would the second use harm a likely or actual licensing market for the original work?). A court will weigh these four factors in light of copyright's fundamental purpose of fostering creativity and innovation, and, in many cases, the public interest. This last bit is particularly important now. COVID-19 has created, almost by definition, a new and powerful public interest purpose that must be considered in any fair use analysis.

People are doing things right now that they instinctively *know* are right, are helping people, are giving light, or are simply things they would be able to do in the physical world. In many cases, their instinct is correct, but they don't know they have legal protections. And even when those people have rights and defenses, they may not know how to use them, or have the resources to do it. Fortunately, fair use has a posse at EFF. If you are the target of an unfair infringement allegation, contact EFF and we'll see if the posse can help.

What You Should Know About Online Tools During the COVID-19 Crisis

A greater portion of the world's work, organizing, and care-giving is moving onto digital platforms and tools that facilitate connection and productivity: video conferencing, messaging apps, healthcare and educational platforms, and more. It's important to be aware of the ways these tools may impact your digital privacy and security during the COVID-19 crisis.

Here are a few things you should know in order to make informed decisions about what works best for you and your communities, and ways you can use security and privacy best practices to protect yourself and others.

Free Slacks

EFF has written about Slack's data retention issues when it comes to free versions of the software. With so many mutual aid networks and organizing groups coalescing on Slack to support our communities, it's important that users are aware that the company retains their messages if they're using a free plan—and they can't automatically delete them. By default, Slack retains all the messages in a workspace or channel (including direct messages) for as long as the workspace exists.

If you are using a paid workspace, you can change how many messages are retained in Slack's databases by setting shorter retention periods. If you're using the free version though, that option is not available to you. Additionally, free workspace users only have the ability to search through the most recent 10,000 messages. And while

users can't see messages sent prior to the 10,000-message mark, they are still available to Slack, law enforcement, and any third-party hackers through a data breach. Leaking or sharing of this data could prove catastrophic, especially for groups who are working to provide aid and support for our most at-risk communities.

Zoom Conferencing

The best way to stave off the effects of isolation is to maintain contact with friends, family, and coworkers. Zoom has quickly become a popular option to work and keep in touch with others in the midst of social distancing and shelter-in-place protocols. There are a few things to keep in mind when using Zoom, particularly in instances where users are relying on the conferencing tool for their studies, or for work-related activities.

Attendee Attention-Tracking

The host of a Zoom call has the capacity to monitor the activities of attendees while screen-sharing. This functionality is available in Zoom version 4.0 and higher. If attendees of a meeting do not have the Zoom video window in focus during a call where the host is screen-sharing, after 30 seconds the host can see indicators next to each participant's name indicating that the Zoom window is not active.

Administrators and User Tracking

Zoom allows administrators to see detailed views on how, when, and where users are using Zoom, with detailed dashboards in real-time of user activity. Zoom also provides a ranking system of users based on total number of meeting minutes. If a user records any calls via Zoom,

administrators can access the contents of that recorded call, including video, audio, transcript, and chat files, as well as access to sharing, analytics, and cloud management privileges.

For any meeting that has occurred or is in-process, Zoom allows administrators to see the operating system, IP address, location data, and device information of each participant. This device information includes the type of machine (PC/Mac/Linux/mobile/etc), specs on the make/model of your peripheral audiovisual devices like cameras or speakers, and names for those devices (for example, the user-configurable names given to AirPods). Administrators also have the ability to join any call at any time on their organization's instance of Zoom, without in-the-moment consent or warning for the attendees of the call.

Schools Moving to Online Learning

Surveillance shouldn't be a prerequisite for getting an education. But even before more school districts started moving their classes and coursework to digital forums for purposes of social distancing, surveillance has become more and more common in schools. With the advent of COVID-19 and the associated uptick in distributed digital learning, the potential for this surveillance to ramp up is alarming.

This is true from kindergarten all the way through graduate school, though it is most prevalent and insidious in K-12 schools. School administrators are choosing to use tools and tactics that encroach on students' privacy in ways that can break down trust amongst students and their peers, teachers, families, and administrators. Many K-12 schools offer or mandate the use of school-issued devices, and those devices come with pre-installed spyware that monitors all student activities and reports them to school administrators.

Many schools are already experimenting with mass surveillance technologies with no evidence, and no way for concerned parents and students to opt out. If your school is using or is considering using technologies like Bark, GoGuardian, Gaggle, Securly, or Social Sentinel, check out our guide to Privacy for Students. It covers many of the privacy and surveillance concerns that these technologies raise, with ways to minimize the data being tracked, risk mitigation strategies, and advocacy tactics.

Telehealth and Non-HIPAA Platforms

The HHS has altered HIPAA rules during the COVID-19 crisis, allowing health care providers to use applications such as FaceTime, Facebook Messenger, Hangouts, Skype, Zoom, etc so they are able to provide care to patients remotely:

During the COVID-19 national emergency, which also constitutes a nationwide public health emergency, covered health care providers subject to the HIPAA Rules may seek to communicate with patients, and provide telehealth services, through remote communications technologies. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules.

If your healthcare provider is using an application or platform that is not covered under HIPAA, check with them on what safeguards they have in place to ensure your privacy is protected, and what their plans and timelines are for moving to platforms that do fall under HIPAA compliance.

Tools for Assessing Risk and Staying Safe Online

One of the best things you can do to keep yourself and others safe during this crisis is to learn how to minimize risk. Many of the problems presented in this post can be mitigated or circumvented with careful consideration of the risks, employing "privacy as a team sport" tactics, and minimizing the data that corporations, employers, and others can track. Our resource site, Surveillance Self-Defense, is full of practical tips, tools, how-to's, and explainers for communicating safely online. Here's a list of useful guides with concrete steps you can take to get started:

- Evaluate and choose the tools you use to make sure they work for you.
- Learn about best practices for communicating with others and incorporate them into your routines and tools.
- Use a password manager to create strong passwords.
- Ensure that you have two-factor authentication (also known as 2FA) enabled for as many accounts as possible.
- Consider your needs and choose the VPN that's right for you.

And lastly, remember—we're all in this together. Take care of each other by safeguarding each other's physical *and* digital health.

Keeping Each Other Safe When Virtually Organizing Mutual Aid

Communities across the country are stepping up to self-organize mutual aid groups, uniting virtually to offer and coordinate support to those who are in need. In solidarity with the need for physical distancing, many people are organizing online using Google spreadsheets, Google forms, public posts on Twitter and Facebook, and private messages on social media platforms.

There is great beauty and power in this support, but it also puts security concerns in the spotlight: overlooked privacy settings and overbroad collection of personal data can lead to the unintended disclosure of private information that can be used to harm the very people seeking help. Though these efforts may seem like they have equal benefit in helping connect people in need to people with resources, the privacy and security implications for these mediums vary widely.

At EFF, we've been approached by U.S.-based mutual aid organizers to provide guidance on digital security and privacy considerations for organizers and volunteers, to better protect the communities they work to support. Our hope with this blog post is to provide considerations for those organizing mutual aid efforts, collecting and storing information, and connecting people with needs with people who want to help. However, we've also included some short lists of questions for anyone interested in contributing to, benefiting from, or aggregating information about mutual aid efforts. If you're interested in learning more, keep reading. Our recommendations are below, followed by a detailed walkthrough of digital security considerations for mutual aid organizers.

Here are some security considerations to keep in mind for organizers, which we'll go into in depth in each section of the post:

- **Define your audience** – Who are you trying to reach, how will you reach them, and what will you ask them to do?
- **Collect as little data as possible** – How much data do you actually need to accomplish your goal, and what is most sensitive to your community?
- **Be mindful of permissions, and restrict access where possible** – Does your data need to be public? What can you restrict to a smaller subset of your community?
- **Use encryption in transit and at rest** – What tools are you using, and who can see your data? Is it protected?
- **Think about which companies, people and systems you're trusting with this sensitive data** – Can you connect participants through end-to-end encrypted platforms?

These are all questions that organizers should think through when designing these efforts, that participants should feel empowered to ask organizers about. The information shared in these efforts can be sensitive, and a prime target for potential phishing attempts. It's important that everyone involved in these efforts understand what the risks are and how to minimize them through thoughtful data collection.

Why Data Security Matters When Organizing Mutual Aid

To make these considerations a little more relatable, throughout this post we'll imagine the journey a mutual aid organizer, Layla, might take. Layla recognizes it's urgent to set up an effort to connect people who need financial support to helpers with resources. She decides to set up a website with a corresponding easily viewable document for people to share and promote their needs, and to provide a way to connect further.

But, in doing so, Layla has determined that she wants to protect her community's sensitive data from people with bad intentions. Personal data can be misused in a variety of ways, and there are, unfortunately, a lot of people who want to take advantage of others' vulnerability during these uncertain and stressful times. These are just a few:

Phishing: In learning very specific information about people's circumstances—such as their emails, Venmo or banking information, their real names, their addresses, the circumstances of them asking for aid, their health information, and their stories—bad actors can scam the very people seeking help. In particular, malicious people take advantage of finding as much information they can about their targets to make a more realistic-sounding scam.

Layla will need to think through how to limit how visible this information is, and ensure she is only collecting sensitive data if it's absolutely necessary.

Doxxing vulnerable groups and facilitating targeted harassment: Private information about someone's livelihood, workplace, and home address can be published with the intention of harassing them. This harassment can be digital, financial, and physical. Digital harassment usually takes the form of abusive comments and behavior online. Financial harassment might mean using this information for fraudulent billing. In other cases, attackers have spammed Venmo requests until the user accidentally accepted. Physical harassment can range from stalking to the practice of prank calling the police so they swarm the victim's address ("swatting"). Even under normal circumstances, these activities can endanger someone's livelihood or safety.

They can be even more detrimental for people who are already marginalized or are particularly affected by current events.

As Layla is supporting a community at risk of their private information being used for targeted harassment, she needs to think through how to protect this information from getting in the hands of bad actors.

Government collection: Many governments collect information about citizens at scale. At its most harmful, this collection and sharing of data between government agencies can put already targeted communities even more at risk, especially when someone might already be surveilled (because of their immigration status, sexuality, gender, health, financial insecurity, faith, ethnicity, or political affiliation).

In Layla's case, she especially worries about Immigration and Customs Enforcement further targeting people in her community, and does not want to collect information that could be misused to facilitate raids.

Selling of data: Companies big and small are constantly scraping the web for information about individuals that they can aggregate and sell, such as is done for third-party tracking.

Layla's community members are worried that sharing their information might mean that they wind up on more telemarketing lists, or that multiple companies that they may not know or recognize begin to track them.

These are all hard problems with terrible consequences: an organizer might determine that they are willing to go through substantial

precautions to prevent these bad outcomes, using the principles we outline below.

With all of these potential threats in mind, Layla knows she wants to protect the submitted data, and as someone from a targeted community, she recognizes that the data she is collecting is very sensitive. Using a **security plan** (or "threat modeling") framework, we can brainstorm through the following questions with Layla:

1. What do you want to protect?
2. Who do you want to protect it from?
3. How bad are the consequences if you fail?
4. How likely are these threats?
5. How much trouble are you willing to go through to try to prevent potential consequences?

The following are considerations that can help Layla and those like her answer these questions.

Define Your Intended (And Unintended) Audience

In thinking through questions around building your community's security plan, it can be helpful to define your goals with this effort and scoping for the size of your initiative.

Who are you trying to reach? Is this effort for a neighborhood community (a group of 20 neighbors who know each other), a local community (people within a township or county, up to hundreds), or larger? The considerations for each of these varying sizes have differing security plans.

What can you clearly communicate to people participating in your effort? Plan to establish expectations at the outset—not just for people asking for and giving help, but external parties that may wish to amplify your effort. Currently, there's a large trend of ag-

gregators cross-linking to other mutual aid efforts, and there's a chance that an effort you intended to be more closed off may get more visibility than you intended. Be clear about structuring your asks for this community: think about how you can make the process transparent to someone just joining the effort: when they submit, how many days should they expect for a response? What happens if a response is fulfilled or unfulfilled? What happens to this document and the data within it?

How much data do you need to organize that aid? Different audiences may require different levels of data collection. Which brings us to our next point.

Collect As Little Data As Possible

Connecting people for mutual aid requires you to share some information about the participants. But it's important to be mindful of the sensitivity of certain types of data—especially regarding a person's medical history, location, and identity. Collecting as little data as possible to accomplish your goals helps lower the risk that bad actors will acquire enough information to do harm to those who provided that data.

Certain types of identifying information may be less risky for a community to share than others. Layla, for example, may know that some people in her community worry about exposing their phone numbers publicly, and so opts to only include an email address field in her form. A first name and email address allow her to identify her participants, so she also decides she doesn't need to store their last names. She might also encourage her community to use email addresses that do not include their first and last names. Now, if the data

were to fall into a bad actor's hands, they would have a harder time uniquely identifying each participant.

Thinking about how long you need to keep information is also important. Deleting information that you no longer need is a great safety measure. Some organizers use documents such as spreadsheets to organize one-time efforts where they don't need to keep the data forever.

Since your community may have different needs and concerns, here are some questions you might ask to ensure you're only collecting what's strictly necessary:

- What types of information do you need to accomplish your goal?
- Are there redundancies in the data you're asking for? If so, can you remove some of those fields?
- Which types of data are the most sensitive to your community? Can you ask for a different, less sensitive alternative piece of information, and still achieve your goal?
- At what point can you delete this spreadsheet and the submitted data?

Be Mindful of Permissions, And Transparent About Access

Within a service like Venmo, Facebook posts, or Google Sheets, users can limit visibility by adjusting settings.

For example, people using Venmo might be surprised that all their transactions are public by default. Users can adjust the settings for their transactions to Private, to be visible to the sender and receiver only; however, Venmo always makes the record of who you are interacting with publicly visible. Google products, like Docs and Sheets, can be made private to be only visible to invited email addresses within a trusted community. Facebook posts can be made more private by limiting visibility to certain friends or communities.

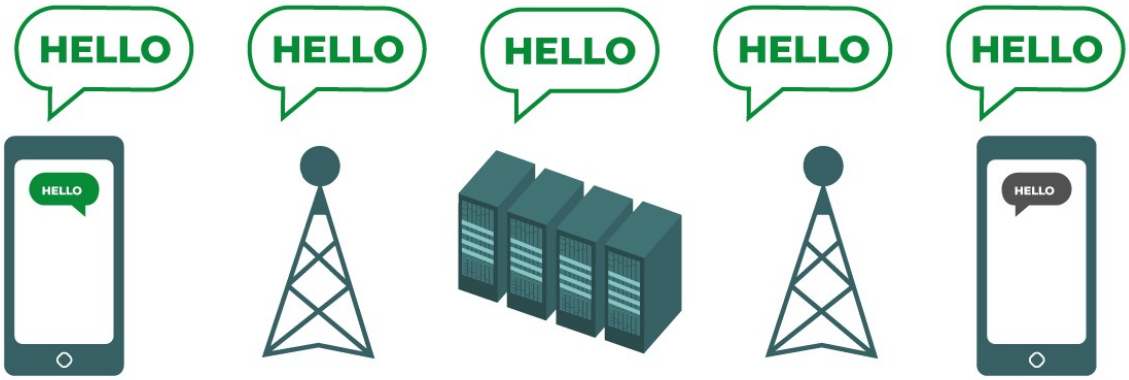
However, permissions and access considerations go beyond individual tools, and organizers need to think them through from the beginning. For example, instead of using a large Google Sheets document that's publicly accessible, visible, and editable by anyone, Layla might consider using a Google Form to have her community submit requests for aid and offers to volunteer. Layla might be comfortable with the minor trade-off that a Google Form requires a few trusted people to vet requests, and she might choose to communicate that process clearly with her community members.

Or perhaps Layla decides to act as matchmaker only—connecting those offering services and those requesting help—by introducing them over email, and encouraging them to use an end-to-end encrypted tool to communicate further details.

Encrypt All The Things

There are many types of encryption, and it's helpful to get familiar with those that are relevant to your mutual aid effort. EFF spends a lot of time writing about the vast benefits of encryption. You can read a more thorough summary on types of encryption at our beginner-friendly educational resource, Surveillance Self-Defense.

When selecting a method to facilitate communication, it's helpful to think through who can see what data, and how that data is stored and protected. When accessing a service through the Internet, your traffic (and all its submitted content—"data"—and information about the content—"metadata") is passed through multiple devices controlled by multiple entities before arriving at the intended destination device. It can be very distressing to learn that information that was intended for one person was in fact visible to many people.



The diagram shows unencrypted data in transit—which is often the default setting for Internet service providers. On the left, a smartphone sends a green, unencrypted message to another smartphone on the far right. Along the way, a cellphone tower passes the message along to company servers and then to another cellphone tower, which can each see the unencrypted "Hello" message. All computers and networks passing the unencrypted message are able to see the message. At the end, the other smartphone receives the unencrypted "Hello" message.

One thing to think about is *how* the data is moving in transit: how are people sharing the information, how are they communicating their needs and services, how are they contacting each other? And how can you make it as safe as possible?

In general, **end-to-end encryption** is the best option available to protect communications data to be between just sender and recipient, as it encrypts between the users' "end" devices. Examples of end-to-end encrypted messaging tools include Signal, WhatsApp, and Keybase. However, before joining an end-to-end encrypted service,

the community needs to hear about this mutual aid effort in the first place, and they might first learn about it through a website.

Which brings us to our next point: **be wary of services and websites that aren't encrypted.** For example, if a service is just using HTTP (and not HTTPS) to collect information submitted from a form, this means their sensitive data is not encrypted.

If you're someone who is running a website, like Layla, you can get a free HTTPS certificate through Let's Encrypt. Check out this list of web hosts that provide HTTPS certificates to see how to get a free Let's Encrypt certificate and provide basic security for your users.

For those hoping for assistance from a mutual aid effort, be wary of services that don't use encryption. Know that mutual aid efforts that encourage you to send very personal information over HTTP offer no protections: anyone from your Internet Service Provider to someone passively looking at your network or the website provider's network can access the data that is submitted. Instead of HTTP, **look for services using HTTPS**, which means that the data is using transport-layer encryption.

Thinking About Trust And The Sensitivity of Your Community's Data

The good news is that most services on the web use HTTPS to protect that data in transit. However, this doesn't necessarily mean that the service deserves your trust. Is it someone who you know personally, running their own website for mutual aid efforts? Do you trust them to protect the data being submitted? Or is it a large company, like

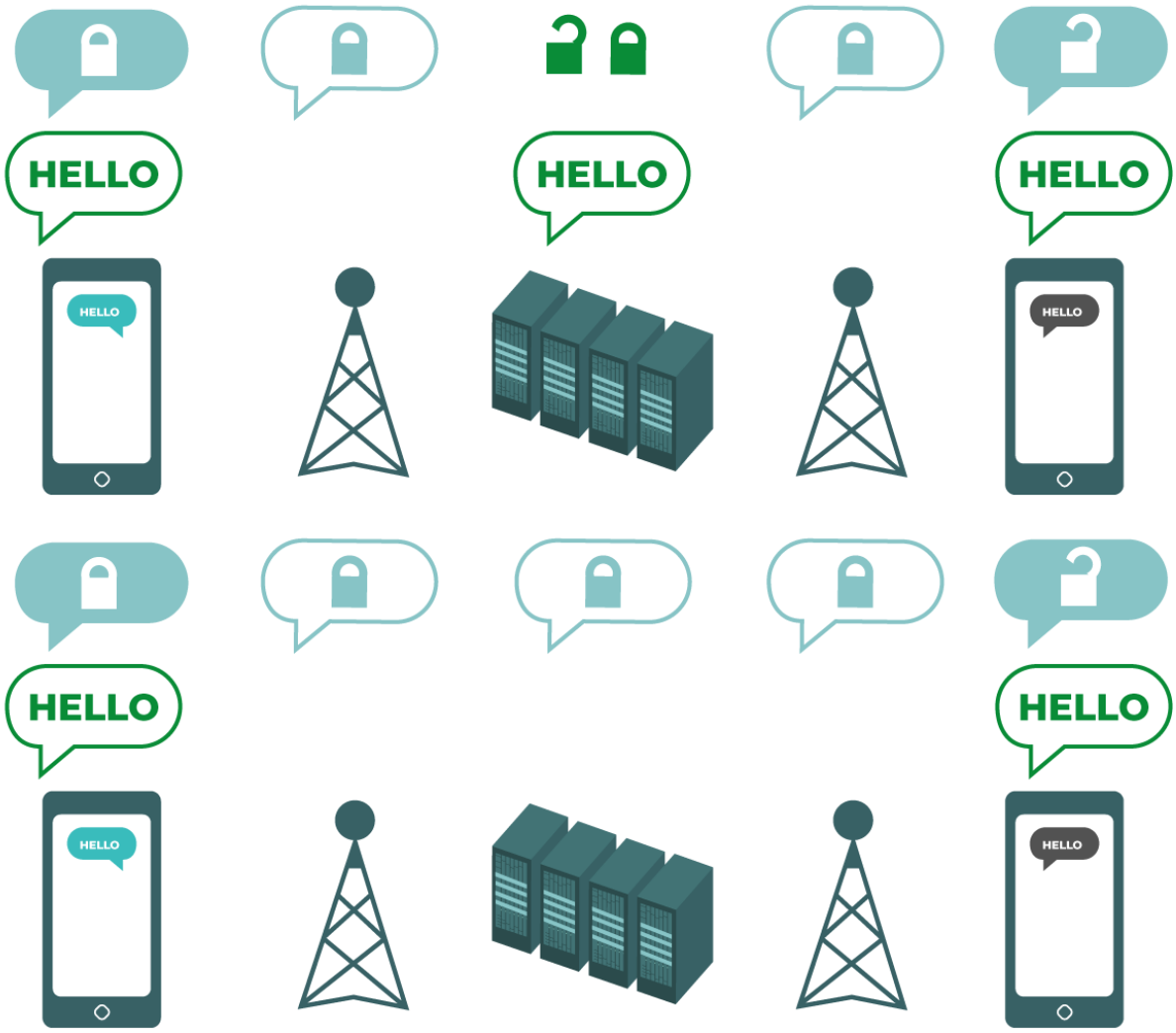
Google, Facebook, or Twitter? Does the company provide different settings for documents and posts, such as “public,” “private,” or restricted to a small group?

In particular, ask yourself the following questions:

- How sensitive is the data that you’re collecting on this platform?
- Do you trust in the security capacity of the service provider?
- Do you trust they'd handle your community’s data responsibly?
- What do you do if you don't trust them?

For some people’s security plans, knowing that a large company like Google or Facebook can see all their communications within the platform is an acceptable risk—for others, this may be completely inappropriate for their community and would violate trust. Those people may instead choose to go with a more privacy-protecting product or to use an end-to-end encrypted service. For more detail on how to consider a service, check out these questions for assessing a vendor’s data security.

Regardless, organizers will want to think about how to facilitate communication *outside* of a company’s service and view. That is, moving from just transport-layer encryption like HTTPS, where the company or website provider can see communications happening on the platform, to an end-to-end encrypted service, where those communications can just happen between the intended sender and intended recipient.



The top diagram demonstrates transport-layer encryption, where a company's devices in the middle can decrypt messages exchanged between users; The bottom diagram demonstrates end-to-end encryption, where the decrypted message is only visible to the end devices and not the service providing devices.

Layla might encourage her community to use a tool like Signal or WhatsApp to communicate more details of their story, as she has determined that she doesn't need to collect nor know this private information.

Other Things To Consider

As Layla's organizing effort gains traction, she may consider cross-linking to other mutual aid organizing efforts to amplify their work. However, each organizing effort has different security plans, and may have different levels of comfort with publicity, or with being cross-linked as a national network of mutual aid efforts. For folks creating these aggregating documents, it's a good practice to ask each of these organizers individually if they're okay with their effort being amplified.

Additionally, aggregators may want to consider the difference between types of information a mutual aid organizer publishes. It may range from the very sensitive (information about community members and requests and offers for help), to less sensitive, such as amplifying government financial assistance programs, or hospital calls to donate Personal Protective Equipment, restaurants offering takeout, and store hours for people with disabilities and the elderly.

For those aggregating and compiling mutual aid efforts, think through:

- Why are you aggregating? What is your goal?
- What different kinds of data or information are you amplifying? Do they need different privacy considerations?
- What information do you **actually** need for your data aggregation to be useful to people?
- Before linking to smaller data sources, can you communicate with the spreadsheet organizers? It's helpful to get consent from the mutual aid organizers you are referencing, as they may not have intended for their work to be viewed beyond their communities.

It's incredible what mutual aid organizers have been able to accomplish in such a short span of time, especially in a time of such up-

heaval. Sites aggregating hundreds of local community resources have cropped up, connecting and supporting people in ways that may prove to be life-saving during this crisis. It's more important than ever to ensure that mutual aid efforts are protective of the people they're serving. Working security planning processes into your organizing is one way to make sure you've got the bases covered for you and your community.

* * *

Participating in Mutual Aid? Keep the Following in Mind

Collecting and sharing information

For those organizing mutual aid, collecting information from individuals, and creating solutions to connect people:

- **Define your audience**
  - Who are you trying to reach? What expectations can your audience have about what's needed from them, how they'll receive updates, and the visibility of their data? Who shouldn't have access to this information?
- **Collect as little data as possible**
  - What minimum data do you need to accomplish your goal? Which types of data are the most sensitive to your community? Can you ask for alternative types of data instead?
- **Be mindful of permissions, and restrict access where possible**
  - Do you need public access to your data? If not, can you restrict permissions to a smaller subset of your community?
- **Use encryption in transit and at rest**
  - For the service or platform you're using, who can see what data? Is your data protected when it's sent or stored?
- **Think about which companies, people, and systems you're trusting with this sensitive data**

    - Can you suggest more secure channels for following up with more detailed information?
    - Can you connect participants through end-to-end encrypted platforms? End-to-end encrypted communications help to protect communications' data to be between the intended sender and intended recipient. Some examples are Signal, Whatsapp, and Keybase.

For those aggregating and compiling mutual aid efforts, think through:

- Why are you aggregating? What is your goal?
- What different kinds of data or information are you amplifying? Do they need different privacy considerations?
- What information do you actually need for your data aggregation to be useful to people?
- Before linking to smaller data sources, can you communicate with the spreadsheet organizers? It's helpful to get consent from the mutual aid organizers you are referencing, as they may not have intended for their work to be viewed beyond their communities

Using and contributing to mutual aid services

For those using and contributing to these mutual aid services, check for clear communication from the organizer about:

- What expectations are for participation in this mutual aid effort
- Which information is necessary or not necessary to participate
- Whether the platform (website form, spreadsheet, or other method) is using encryption, and ensure that it is at least using HTTPS
- How publicly visible the data is, and how much organizers can see versus the general public
- Where the data will be stored, and for how long
- Whether there are end-to-end encrypted communication tools for connecting with participants further around sensitive details, and how to separate those details from a more widely-viewed platform

Additional considerations for people participating in mutual aid efforts are:

- Know your risks: can you communicate these concerns with the organizers and talk through the steps they are taking to mitigate them?
- Be wary of potential phishing attempts relating to the information provided.
- Consider what you can omit: Do you need to give out your real name, or other identifying information such as your phone number or home address? If your email includes your real name, can you use a different email that's less connected to your identity?

We'd like to thank Sherry Wong, Rocket Lee, Mona Wang and Martin Shelton for their guidance.

Afterword

These articles were written by the lawyers, technologists and activists of EFF while living, as millions of others have been, under quarantine, shelter in place orders, or just staying home to voluntarily help protect our communities. In these times of physical separation from other people, we rely on the Internet and digital tools to share information and advice, create art and memes, listen to our favorite musicians perform "live," or just to feel less alone. Technology is helping us cope with the loss of in-person contact. Others are using digital tools and services to organize mutual aid for their neighborhoods and communities in this time of crisis.

Thanks to open access science, scientific and medical teams are able to instantly share their work and build on efforts to track the virus, study its effect on people, and develop vaccines. Others are developing ways to create and repair vital medical equipment using open tools, including 3D printing. We are coming together online in new and creative ways, and ensuring that security, privacy, and openness are baked into the tools and services we use.

The explosion of open creativity online to keep us connected and sane during these scary times is one of the bright spots in the darkness. But it also shows how this crisis disproportionately impacts those of us who are marginalized in society already—the unsheltered, those who cannot afford or access reliable broadband service to continue school or work, the retail workers who have little reserves, and all of those falling through our frayed social safety net. Innovation is needed here too—like ensuring that robust broadband access works

for everyone, not just the wealthy, and is not dependent on temporary largess of giant providers.

We Must Be Extra Vigilant In Defending Our Rights In This Moment

Times of great public fear come with great risk. Public fear has driven some of the worst human rights atrocities, and given opportunities for those who would seize power from us and reduce or even erase our hard-won human rights and civil liberties. We have seen efforts to place irrational blame for this public health crisis on Asian communities and direct even more pressure and discrimination against refugees and immigrants. We see calls from companies seeking to cash in on this crisis for unchecked face surveillance and other efforts far beyond what medicine or epidemiology require.

When fear threatens to undermine our rights and pervert justice, that's where EFF—and you—come in.

This virus requires us to take steps that would be unthinkable in normal times, like staying inside. But we must be vigilant. We must be sure that measures taken in the name of responding to COVID-19 are, in the language of international human rights law, "necessary and proportionate" to the needs of society in fighting the virus. Above all, we must make sure that these measures end and that any data collected for these purposes is not re-purposed for either governmental or commercial ends.

We Can Take Advantage Of Technology, and Emerge Stronger

EFF is standing strong to make sure that we take advantage of how technology can help us now, and emerge from this time with our freedom and democracy as strong, if not stronger, than when we went in. Because we at EFF have a committed membership as our primary support–over half of our annual budget comes from individuals—we have been able to pivot our attention to these issues even as we continue our ongoing fights. Our lawyers are scrutinizing laws and regulations and corporate privacy moves, especially the growing and concerning raft of corporate/government surveillance efforts. Our technologists are digging into the digital tools we all rely on to make sure that your privacy is protected. We're pushing to lower artificial barriers to information sharing, and working to make sure that access to knowledge is one of the things we keep as we emerge from these times.

Right now, when real science is so often under attack, those of us who care about truth, health, and each other need to take seriously the things that science and medicine are telling us about how to keep this virus from spreading. And we also need to be vigilant so that we come out the other side of this crisis with a society we want to live in and hand down to our kids. We can—and must—do both.

Cindy Cohn
May 4, 2020